Ante la

Corte Interamerican de Derechos Humanos

———————♦———————

Caso Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo"

v.

República de Colombia

———————♦———————

Escrito de *Amici Curiae* de Article 19, Electronic Frontier Foundation, Fundación Karisma, and Privacy International

———————♦———————

ROXANNA ALTHOLZ
INTERNATIONAL HUMAN RIGHTS LAW CLINIC
UNIVERSITY OF CALIFORNIA, BERKELEY, SCHOOL OF LAW
353 Law Building
Berkeley, CA 94720
(510) 643-8781
raltholz@law.berkeley.edu

ASTHA SHARMA POKHAREL
INTERNATIONAL HUMAN RIGHTS LAW CLINIC
UNIVERSITY OF CALIFORNIA, BERKELEY, SCHOOL OF LAW
353 Law Building
Berkeley, CA 94720
+1 (510) 642-4139
asharmapokharel@clinical.law.berkeley.edu

Asesores Jurídicos de Amicus Curiae

Índice

I. CITAS DE LA DOCTRINA Y LA JURISPRUDENCIA

CASOS

TEXTOS LEGALES

INFORMES DE INSTANCIAS INTERNACIONALES DE DERECHOS HUMANOS

<u>LIBROS, ARTICULOS E INFORMES DE ONGS</u>

II. INTERÉS DE LOS *AMICI CURIAE*

ARTICLE 19 es una organización internacional de derechos humanos con sede en Londres (institución de beneficencia inscrita en el Reino Unido con el número 32741) y varias oficinas regionales, entre ellas ARTICLE 19 México y Centroamérica y ARTICLE 19 Brasil y Sudamérica. La organización toma su nombre y su mandato del artículo 19 de la Declaración Universal de Derechos Humanos, que garantiza el derecho a la libertad de opinión y de expresión. ARTICLE 19 lucha contra la censura en todas sus formas en todo el mundo. Con los años, ha elaborado varios documentos que han servido de fuente para el establecimiento de normas, así como escritos sobre políticas públicas, basados en el derecho internacional, el derecho comparado y las mejores prácticas en el ámbito de la libertad de expresión, incluso sobre temas relacionados con la libertad de expresión y la vigilancia. Con frecuencia, ARTICLE 19 presenta comentarios escritos y *amicus curiae* en casos en los cuales se plantan cuestiones vinculadas a la garantía internacional de la libertad de expresión ante tribunales regionales —como la Corte Interamericana de Derechos Humanos, el Tribunal Europeo de Derechos Humanos y la Corte Africana de Derechos Humanos y de los Pueblos— y tribunales de jurisdicción nacional.

La **Electronic Frontier Foundation (EFF)** es una organización civil internacional sin fines de lucro dedicada a la defensa de la libertad de expresión, la privacidad y la innovación en el mundo digital. La EFF defiende los derechos humanos de los usuarios en el ámbito digital por medio de litigios de alto impacto, análisis de políticas, el activismo de base y el desarrollo de la tecnología. El gran interés de la EFF en este caso se debe a su trabajo de larga data para combatir la vigilancia arbitraria o abusiva y promover la aplicación de normas internacionales de derechos humanos al acceso del gobierno a datos sobre comunicaciones. La EFF estuvo a la vanguardia de la coalición mundial que formuló los *Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones* en 2014. Estos principios se han citado en numerosos documentos, entre ellos informes de relatores especiales sobre la libertad de expresión de las Naciones Unidas y de la Comisión Interamericana de Derechos Humanos. La EFF ha trabajado también con otras organizaciones de América Latina con el fin de mejorar las prácticas de los proveedores de servicios de Internet para proteger mejor la privacidad y fomentar la transparencia en el acceso del gobierno a datos de los usuarios.

La **Fundación Karisma** es una organización colombiana sin fines de lucro dedicada a la protección y la promoción de los derechos humanos y la justicia social en el diseño y el uso de tecnologías digitales. Karisma trabaja en cuatro líneas programáticas: 1) democratización de los conocimientos y la cultura, 2) participación cívica, 3) autonomía y dignidad, 4) inclusión social. Además, tiene dos laboratorios especiales: uno sobre seguridad digital y privacidad, conocido como K+LAB, y K-Apropiación Tecnológica, que trabaja con las comunidades para abordar retos planteados por la tecnología.

Privacy International (PI) es una organización no gubernamental sin fines de lucro, con sede en Londres (institución de beneficencia número 1147471), que realiza una labor de investigación y promoción en todo el mundo contra los abusos de los datos y la tecnología cometidos por gobiernos y empresas. Expone los daños y los abusos, moviliza aliados a escala mundial, lleva a

cabo campañas con el público para buscar soluciones y presiona a empresas y gobiernos a fin de impulsar cambios. PI cuestiona la vigilancia con un alcance excesivo por parte del Estado y las empresas, a fin de que, en todas partes, la gente goce de más seguridad y libertad como consecuencia de una mayor privacidad personal. En esta gama de actividades, PI investiga la forma en que se generan y se usan datos personales y cómo se los puede proteger por medio de marcos jurídicos y tecnológicos. PI ha asesorado y presentado informes a organizaciones internacionales tales como el Consejo de Europa, el Parlamento Europeo, la Organización de Cooperación y Desarrollo Económicos, el Alto Comisionado de las Naciones Unidas para los Derechos Humanos y el Alto Comisionado de las Naciones Unidas para los Refugiados.

III. RESUMEN DEL ARGUMENTO

Los *amici curiae* presentan este escrito a la Honorable Corte Interamericana de Derechos Humanos ("la Corte Interamericana" o "la Corte") a fin de examinar la forma en que, a pesar de las reformas jurídicas en materia de inteligencia efectuadas desde 2013, las autoridades colombianas han interceptado de manera sistemática e ilegal comunicaciones de la Corporación Colectivo de Abogados José Alvear Restrepo (CCAJAR). En este escrito, los *amici curiae* demuestran que la vigilancia ilegal de las comunicaciones efectuada por órganos de inteligencia del Estado vulnera una amplia gama de derechos humanos, lo cual socava las piedras angulares de las sociedades democráticas. Los *amici curiae* afirman que los agentes de inteligencia colombianos vigilaron ilegalmente las comunicaciones de miembros de la CCAJAR en un marco jurídico que no se ciña a las normas internacionales de derechos humanos.

Colombia ha montado un sistema extenso e invasivo de vigilancia de las comunicaciones y lo ha usado en contra de defensores de derechos humanos con el fin de desalentar e impedir su trabajo en el campo de los derechos humanos. Los órganos de inteligencia recurrieron a la vigilancia de las comunicaciones para recopilar información personal sobre miembros de la CCAJAR y sus familiares en violación del derecho a la privacidad y de otros derechos humanos. En la era digital, el derecho a la privacidad se ha convertido en una condición previa para la protección de otros derechos —como el derecho a la vida y a la integridad personal— y de la libertad de asociación, de expresión y de circulación. En este caso, los métodos de vigilancia ilegales utilizados por el Estado infringieron también los derechos de los hijos de miembros de la CCAJAR.

En 2013 se promulgó en Colombia la Ley Estatutaria 1621 de 2013 ("la Ley de Inteligencia de 2013" o "la Ley de Inteligencia") para responder a las revelaciones efectuadas en los medios de comunicación de que los órganos de inteligencia del país perseguían de manera sistemática e ilegal a defensores de derechos humanos y periodistas, entre ellos miembros de la CCAJAR. Colombia afirma ante esta Corte que las disposiciones de la Ley de Inteligencia "establece de manera clara y precisa las circunstancias concretas en que [las labores de inteligencia] pueden ser autorizadas para garantizar que toda actuación se ajuste a los principios de legalidad, proporcionalidad y necesidad" y que "dispone controles en varios niveles frente el desarrollo" de actividades de inteligencia[1]. Contrariamente a las aseveraciones del Estado, desde que se aprobó la Ley de Inteligencia, los órganos de inteligencia han vigilado, acosado y atacado

---

[1] Corte IDH, Audiencia Pública del Caso Miembros Corporación Colectivo de Abogados CAJAR vs. Colombia Parte 2, 8:32:28-8:32:49, YOUTUBE (13 de mayo de 2022), https://youtu.be/8Fiv0Hcl86o.

de forma sistemática e ilegal a la CCAJAR, lo cual ha vulnerado sus derechos y ha tenido consecuencias perniciosas para los derechos de las personas y las comunidades que defienden. A fin de sopesar las actividades de inteligencia y el marco jurídico vigente, esta Corte debe examinar las normas de legalidad, legitimidad, necesidad y proporcionalidad, así como las salvaguardias procesales establecidas en la Convención Americana sobre Derechos Humanos ("la Convención Americana").

Como los Estados están recurriendo en medida creciente a innovaciones tecnológicas para monitorear la vida de las personas de formas sumamente invasivas, este caso ofrece una oportunidad sin precedentes para que esta Corte determine si el régimen jurídico de Colombia y los métodos utilizados por los servicios de inteligencia del país son compatibles con la Convención Americana y aclare las protecciones jurídicas con que cuentan los defensores de derechos humanos contra la vigilancia estatal. Al aclarar la aplicación de las normas interamericanas a la vigilancia de las comunicaciones, que se ha vuelto común en la región, esta Corte ofrecerá remedio y protección a la CCAJAR y a otros defensores de derechos humanos frente a futuras violaciones y reforzará las protecciones para las personas y las organizaciones perseguidas por el Estado por su labor de legítima defensa de los derechos humanos.

IV. ARGUMENTO

A. LA VIGILANCIA ILEGAL Y ARBITRARIA POR EL ESTADO VULNERA UNA AMPLIA GAMA DE DERECHOS HUMANOS PROTEGIDOS POR LA CONVENCIÓN AMERICANA EN DETRIMENTO DE LA SOCIEDAD DEMOCRÁTICA

Los órganos de inteligencia, a menudo de manera encubierta, recopilan, analizan, monitorean, evalúan y utilizan información obtenida de personas y organizaciones tanto del país como extranjeras con fines de seguridad nacional, entre otros[2]. Los órganos de inteligencia colombianos han vigilado ilegalmente a candidatos políticos, jueces, fiscales, periodistas y defensores de derechos humanos, alegando que se trataba de una cuestión de seguridad nacional[3]. En este escrito se examina el uso de la vigilancia secreta dentro del país por órganos de inteligencia colombianos a fin de obtener información sobre estos grupos de manera arbitraria, al margen del derecho internacional y la legislación interna.

En 2013, un tribunal colombiano describió al principal órgano de inteligencia de Colombia, el Departamento Administrativo de Seguridad (DAS), de la siguiente forma:

> ... la materialización de una verdadera asociación criminal concebida de antemano y dirigida a la comisión de delitos indeterminados que después se concretaron en violación ilícita de comunicaciones, utilización de equipos transmisores o receptores en concurso sucesivo y homogéneo y abuso de autoridad por acto

---

[2] Consejo de Derechos Humanos, *Informe de Martin Scheinin, Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo: Recopilación de buenas prácticas relacionadas con los marcos y las medidas de carácter jurídico e institucional que permitan garantizar el respeto de los derechos humanos por los servicios de inteligencia en la lucha contra el terrorismo, particularmente en lo que respecta a su supervisión*, Práctica 2, U.N. Doc. A/HRC/14/46 (17 de mayo de 2010) [en adelante "Informe de 2010 del Relator Especial sobre la protección y la promoción de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo"

[3] Véase, por ejemplo, CIDH, Informe No. 57/19, párr. 159, Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo", Colombia, Caso 12.380, OEA/Ser.L/V/II.172, Doc. 66.

> arbitrario e injusto, con el propósito final de obtener, procesar y analizar información privada de ONGS, abogados defensores de derechos humanos, colectivos de abogados, periodistas y en fin personas con tendencia o ideología opositora o contradictoria al gobierno nacional de turno...[4].

Numerosos órganos y expertos internacionales, entre ellos esta Corte, han vinculado de manera directa operaciones de inteligencia realizadas por órganos de inteligencia colombianos a actos de intimidación y violencia cometidos por agentes estatales y no estatales[5]. Colombia se ha ganado la dudosa distinción de ser uno de los países más peligrosos del mundo para los defensores de derechos humanos[6]. En 2018, por ejemplo, 40% de los asesinatos de defensores de derechos humanos perpetrados en todo el mundo se produjeron en Colombia[7]. La vigilancia ilegal ha colocado a los defensores de derechos humanos en la mira y ha exacerbado su riesgo de violencia.

Por lo menos desde 1999, Colombia ha usado su extensiva red de vigilancia para monitorear a miembros de la CCAJAR, así como a sus familiares, y compilar información sobre todas las facetas de su vida profesional y familiar, incluidos sus movimientos y actividades profesionales y personales, su situación financiera, sus viajes, sus contactos, sus clientes y sus sistemas de protección. No cabe duda de que la vigilancia de las comunicaciones de miembros de la CCAJAR y sus familiares violó sus derechos a la privacidad, a la vida y a la integridad

---

[4] Comisión Interamericana de Derechos Humanos (CIDH), *Verdad, justicia y reparación: Cuarto informe sobre la situación de derechos humanos en Colombia*, párr. 959, OEA/Ser.L/V/II, Doc. 49/13 (31 de diciembre de 2013) [en adelante *Verdad, justicia y reparación*] (donde se cita la decisión del Juzgado Tercero Penal del Circuito Especializado de Descongestión de Bogotá).

[5] Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (ACNUDH), *Mandatos del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión; de la Relatora Especial sobre ejecuciones extrajudiciales, sumarias o arbitrarias; de la Relatora Especial sobre la situación de los defensores de derechos humanos; del Relator Especial sobre la promoción de la verdad, la justicia, la reparación y las garantías de no repetición; y del Relator Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la Organización de los Estados Americanos*, AL COL 5/2020 (15 de junio de 2020) (donde se expresa preocupación acerca de las actividades de inteligencia militar, entre ellas la vigilancia y el seguimiento de defensores de derechos humanos); CIDH, Informe No. 57/19, *supra*, nota 3, párr. 296 (donde se recalca que "las labores de inteligencia del DAS tenían fines ilegítimos e inconvencionales, que incluyeron entregar la información recabada sobre los miembros del CAJAR a grupos paramilitares"); Comité de Derechos Humanos, *Observaciones finales del Comité de Derechos Humanos. Colombia*, párr. 16, U.N. Doc. CCPR/C/COL/CO/6 (4 de agosto de 2010) [en adelante *Observaciones finales del Comité de Derechos Humanos sobre Colombia (2010)*] (donde se señala el involucramiento de agentes de inteligencia en amenazas y en la vigilancia de jueces y se afirma que Colombia "debe crear sólidos sistemas de control y supervisión sobre los organismos de inteligencia y crear un mecanismo nacional de depuración de los archivos de inteligencia, en consulta con víctimas y organizaciones interesadas"); Corte Interamericana de Derechos Humanos (Corte IDH), Caso Manuel Cepeda Vargas vs. Colombia, Sentencia de 26 de mayo de 2010 (Excepciones Preliminares, Fondo, Reparaciones y Costas), serie C, No. 213, párr. 216 (donde se dispone que Colombia debe investigar a los responsables de la ejecución extrajudicial de la víctima, así como la presunta participación de agentes de inteligencia); ACNUDH, *Informe anual de la Alta Comisionada de las Naciones Unidas para los Derechos Humanos sobre la situación de los derechos humanos en Colombia*, párrs. 14 y 15, U.N. Doc. A/HRC/13/72 (4 de marzo de 2010) (donde se señala que las actividades de inteligencia ilegales dirigidas contra defensores de derechos humanos "incluyeron interceptaciones de teléfonos y correos electrónicos, seguimientos, hostigamientos y amenazas, robos de información e ingresos ilegales a oficinas y domicilios"); Comité contra la Tortura, *Observaciones finales del Comité contra la Tortura. Colombia,* párr. 15, U.N. Doc. CAT/C/COL/CO/4 (4 de mayo de 2010) (donde se insta a Colombia "a que tome medidas inmediatas para discontinuar el acoso y seguimiento de jueces por agentes del DAS").

[6] Consejo de Derechos Humanos, *Visita a Colombia. Informe del Relator Especial sobre la situación de los defensores de los derechos humanos*, párr. 20, U.N. Doc. A/HRC/43/51/Add.1 (26 de diciembre de 2019). En Colombia, tras la firma del Acuerdo de Paz con las FARC-EP en 2016, los actos de violencia contra defensores de derechos humanos se "han incrementado sostenidamente". CIDH, *Informe sobre la situación de personas defensoras de derechos humanos y líderes sociales en Colombia*, párr. 42, OEA/Ser.L/V/II 29 (2019) [en adelante *Personas defensoras de derechos humanos en Colombia*].

[7] FRONT LINE DEFENDERS, ANÁLISIS GLOBAL DE FRONTLINE DEFENDERS 2018, https://www.frontlinedefenders.org/sites/default/files/spanish_annual_report.pdf.

personal, además de la libertad de asociación, de expresión y de circulación y los derechos del niño.

La vigilancia de miembros de la CCAJAR y sus familiares, así como las afectaciones resultantes de derechos humanos, se han intensificado en grado y en escala como consecuencia del uso de tecnología de vigilancia avanzada.

1. Colombia ha establecido un sistema extenso de vigilancia de las comunicaciones con amplia capacidad técnica

En el curso de los sesenta años de guerra en el país, Colombia ha establecido un aparato de inteligencia formidable, con capacidad de vigilancia masiva. En 2011, la Dirección Nacional de Inteligencia (DNI) reemplazó al DAS como principal órgano de inteligencia en Colombia, tras las revelaciones de que los agentes del DAS habían realizado un espionaje sistemático de críticos y opositores políticos y habían conspirado con fuerzas paramilitares de derecha para asesinar a defensores de derechos humanos. Además de la DNI, hay unidades de inteligencia en el Ejército Nacional, la Armada, la Fuerza Aérea, la Policía Nacional, el Comando General de las Fuerzas Militares y la Unidad de Información y Análisis Financiero. Estos órganos de inteligencia están bajo intensa presión para producir inteligencia y están compitiendo constantemente por recursos y herramientas de vigilancia[8].

Los órganos de inteligencia utilizan una amplia gama de métodos para vigilar las comunicaciones[9]. Como se describe con más pormenores en el apartado B.1.b, aunque en el derecho internacional se permite la vigilancia específica en circunstancias limitadas y con estrictas salvaguardias, la vigilancia masiva interfiere de manera intrínsecamente desproporcionada en el derecho internacional a la privacidad. En los últimos años, las fuerzas de seguridad y los servicios de inteligencia de Colombia han adquirido herramientas para ampliar su extensa red de espionaje y captar grandes cantidades de datos de las comunicaciones[10]. En este apartado se describe la capacidad tecnológica desarrollada por Colombia para buscar, recopilar y retener de manera ilegal y arbitraria cantidades masivas de información personal sobre individuos, entre ellos miembros de la CCAJAR y sus familiares.

Colombia utiliza herramientas de vigilancia específica y masiva. Las autoridades recopilan, monitorean e interceptan comunicaciones individuales de audio y de datos en tiempo real de teléfonos móviles y fijos. La administración del sistema, establecido en 2000 y conocido como "Proyecto Esperanza", está a cargo de la Fiscalía General de la Nación. Las interceptaciones por medio de este sistema deben ser solicitadas por escrito por un analista, con

---

[8] PRIVACY INTERNATIONAL, UN ESTADO EN LA SOMBRA: VIGILANCIA Y ORDEN PÚBLICO EN COLOMBIA 7, 39 (2015), https://privacyinternational.org/sites/default/files/2017-12/ShadowState_Espanol.pdf [en adelante ESTADO EN LA SOMBRA].

[9] Consejo de Derechos Humanos, *Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Frank La Rue*, párr. 6.a, U.N. Doc. A/HRC/23/40 (17 de abril de 2013) [en adelante "Informe de 2013 del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión"].

[10] Los datos de las comunicaciones consisten en "la información acerca de las comunicaciones personales (correos electrónicos, llamadas telefónicas y mensajes de texto enviados y recibidos, mensajes y publicaciones en redes sociales), identidad, cuentas de usuarios de red, direcciones, sitios web visitados, libros y otro material consultado, mirado o escuchado, búsquedas realizadas, recursos utilizados, interacciones (origen y destino de las comunicaciones, personas con las que se interactuó, amigos, familiares, conocidos), y horario y ubicación del usuario, incluida la proximidad con otras personas". *Id.*, párr. 6.b.

autorización de la Fiscalía General, y deben ser objeto de revisión previa o autorización por un juez dentro de un plazo de 36 horas[11]. Sin embargo, hay evidencia de que el DAS usó la tecnología del Proyecto Esperanza para interceptar datos telefónicos sin autorización previa o supervisión judicial y proporcionó la información obtenida por medio de este sistema a grupos paramilitares[12].

Aunque las autoridades colombianas afirmaban que el sistema del Proyecto Esperanza era el único que usaban las fuerzas de seguridad para interceptar comunicaciones, en 2015 se reveló que la Dirección de Inteligencia Policial (DIPOL) tenía acceso directo a redes o sistemas de comunicaciones. Por medio del Sistema Integrado de Grabación Digital (SIGD), la policía podía interceptar señales de comunicaciones, tanto por internet como telefónicas, que viajan "a través de sondas de red conectadas a una plataforma para centro de monitoreo llamada Sistema Integral de Grabación Digital (SIGD)"[13]. El SIGD "se concibió para ir más allá de la interceptación de 'blancos preasignados' y recopilar tráfico 'masivo' de comunicaciones en 16 líneas troncales y generar nuevos blancos"[14]. Los datos se procesan en centros de monitoreo con "potentes ordenadores que muestran conexiones entre personas, sus conversaciones y eventos, y elaboran perfiles de las personas y sus contactos"[15]. La policía abusaron del sistema al vigilar las comunicaciones de periodistas que investigaban actos de corrupción y conducta sexual inapropiada de la policía, por ejemplo[16].

Las fuerzas de seguridad y los órganos de inteligencia de Colombia también tienen acceso directo a "capacidades de vigilancia masiva del tráfico de Internet"[17]. La Plataforma Única de Monitoreo y Análisis (PUMA), que entró en servicio en 2007 y fue actualizada en 2014, es un sistema de monitoreo telefónico y de internet conectado directamente a la infraestructura de la red de los proveedores de servicios por medio de una sonda que copia grandes cantidades de datos y los envía directamente a un centro de monitoreo[18]. Por medio de PUMA, los órganos estatales pueden interceptar y retener "todas las comunicaciones transmitidas por los cables de alto volumen que componen la troncal de la que todos los

---

[11] ESTADO EN LA SOMBRA*, supra,* nota 8, pág. 23. Véase también Vivian Newman Pont, *Chuzadas legales: Más preguntas que respuestas* (2012), https://www.dejusticia.org/chuzadas-legales-mas-preguntas-que-respuestas/.

[12] Véase, por ejemplo, Rodrigo Silva Vargas, '*Ventilador de la parapolítica' involucra a Luís Camilo Osorio,* CARACOL RADIO (2 de noviembre de 2007), https://caracol.com.co/radio/2007/11/02/nacional/1193982780_501669.html (donde se cita el testimonio del exdirector de información del DAS ante el Congreso de Colombia: "La información del proyecto Esperanza fue enviada por Jorge Noguera [exdirector del DAS], por mi intermedio, a miembros de las Autodefensas").

[13] ESTADO EN LA SOMBRA*, supra,* nota 8, pág. 15.

[14] *Id*., pág. 37.

[15] *Id*., pág. 15.

[16] Adriaan Alsema, *Colombia Police 'Wiretapping, Shadowing and Intimidating Journalists'*, COLOMBIA REPORTS (3 de diciembre de 2015), https://colombiareports.com/colombias-police-wiretapping-and-intimidating-journalists/.

[17] ESTADO EN LA SOMBRA*, supra,* nota 8, pág. 14. Según este informe, "Esperanza permite a la Fiscalía conectarse a los servidores de los proveedores de servicios de telecomunicaciones para recibir y descomponer en paquetes información de llamadas en tiempo real a fin de transmitirla a una sala central de monitoreo. La señal se envía luego a otras salas de monitoreo controladas por el Cuerpo Técnico de Investigación (CTI) de la Fiscalía, la Policía y el DAS, cuando éste estaba operativo". *Id*., pág. 21. Véase también *¿Dónde están mis datos?,* FUNDACIÓN KARISMA 11 (2021), https://web.karisma.org.co/donde-estan-mis-datos-2021/ (donde se afirma que las autoridades colombianas usan tecnología para tener acceso a datos de usuarios de telecomunicaciones por medio de una puerta abierta a la infraestructura de telecomunicaciones de las compañías); *id*., págs. 21 y 22 (donde se señala que las empresas de telecomunicaciones informan que la Fiscalía General tenía acceso directo a datos de usuarios de teléfonos móviles).

[18] FUNDACIÓN KARISMA, FUNDACIÓN KARISMA'S RESPONSE TO CALL FOR INPUT TO A REPORT ON THE RIGHT TO PRIVACY IN THE DIGITAL AGE BY THE UN HIGH COMMISSIONER FOR HUMAN RIGHTS 4 (9 de abril de 2018), https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/Karisma.pdf.

colombianos dependen para hablar entre ellos y enviarse mensajes”[19]. Con PUMA, los servicios de inteligencia pueden interceptar directamente “lo que se hable, escriba o envíe desde correos electrónicos, Facebook, Twitter, Line, Viber, Skype y, en definitiva, todo tipo de comunicación que se realice a través de Internet”[20]. PUMA puede no solo captar el tráfico de comunicaciones de los usuarios, sino también “apropiarse del dispositivo de la persona seleccionada, controlarlo y conocer todo lo que se encuentre allí o en sus inmediaciones”[21]. En 2015, un grupo que monitoreaba la vigilancia de las comunicaciones en Colombia observó que “PUMA está en condiciones de convertirse [...] en el más potente y avanzado sistema de monitoreo masivo de las comunicaciones de Colombia”[22].

Asimismo, los servicios de inteligencia colombianos han llevado a cabo operaciones de intrusión que utilizan software, datos, sistemas informáticos o redes para obtener acceso no autorizado a información y dispositivos de usuarios. Estas estrategias focalizadas consisten en desplegar *malware* (programas maliciosos), *spyware* (programas espía) y dispositivos de monitoreo para recopilar información acerca de determinadas personas[23]. Por ejemplo, los servicios de inteligencia han usado virus troyanos para infectar “el dispositivo del objetivo” y “recopilar sus datos, activar y desactivar a distancia la webcam y el micrófono y copiar archivos y contraseñas tecleadas”[24]. En 2020 los medios revelaron que las Fuerzas Militares de Colombia habían usado un programa malicioso denominado “Hombre invisible” para espiar a funcionarios públicos y defensores de derechos humanos[25].

En operaciones de inteligencia colombianas también se han usado dispositivos para monitorear teléfonos móviles (“simuladores de emplazamiento de célula”, conocidos también como “receptores de identidad internacional de abonado móvil o receptores IMSI”) “que permiten la interceptación localizada indiscriminada de todas las llamadas de teléfonos móviles y mensajes de texto en un lugar específico”[26]. Conocidos comúnmente como “stingrays”, estos

---

[19] ESTADO EN LA SOMBRA*, supra,* nota 8, pág. 27.

[20] *Policía podrá Interceptar Facebook, Twitter y Skype en Colombia*, EL TIEMPO (22 de junio de 2013), https://www.eltiempo.com/archivo/documento/CMS-12890198.

[21] *En Colombia, el PUMA no es como lo pintan,* DIGITAL RIGHTS LAC (2015), https://digitalrightslac.derechosdigitales.org/es/en-colombia-el-puma-no-es-como-lo-pintan/.

[22] ESTADO EN LA SOMBRA*, supra,* nota 8, pág. 31

[23] Se ha comprobado que los servicios de inteligencia militar de Colombia han comprado diversas herramientas de vigilancia. Según la revista *Semana*, en un informe forense presentado a la Corte Suprema de Colombia se describen “varias herramientas informáticas que fueron encontradas en el allanamiento” del Batallón de Ciberinteligencia del Ejército, entre ellas programas maliciosos y herramientas de intrusión. *El informe forense de las carpetas secretas*, SEMANA (12 de mayo de 2020), https://www.semana.com/nacion/articulo/el-informe-forense-de-las-carpetas-secretas/670853/.

[24] ESTADO EN LA SOMBRA*, supra,* nota 8, pág. 43. Véase también Informe de 2013 del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión*, supra,* nota 9, párr. 62.

[25] *Lo que quería el Ejército con ‘Hombre invisible’ que hizo chuzadas reveladas por Semana*, PULZO (14 de enero de 2020), https://www.pulzo.com/nacion/como-funciona-software-hombre-invisible-que-uso-ejercito-para-chuzar-PP828082. Según un suboficial que participó en las interceptaciones ilegales, el “Hombre invisible” le permitía meterse “a cualquier computador, acceder a llamadas y conversaciones de WhatsApp y Telegram Web, descargar conversaciones de chat archivadas o borradas, fotos y, en general lo que tenga almacenado en la memoria de la máquina infectada”, sin dejar rastro. *Id.*

[26] ESTADO EN LA SOMBRA*, supra,* nota 8, pág. 15. Véase más información sobre la capacidad de los simuladores de emplazamiento de célula en Yomna N, *Gotta Catch 'Em All: Understanding How IMSI-Catchers Exploit Cell Networks*, EFF (28 de junio de 2019), https://www.eff.org/wp/gotta-catch-em-all-understanding-how-imsi-catchers-exploit-cell-networks; PRIVACY INTERNATIONAL, IMSI CATCHERS: PI’S LEGAL ANALYSIS (2020), https://privacyinternational.org/report/3965/imsi-catchers-pis-legal-analysis.

dispositivos “transmiten una potente señal inalámbrica que hace que los teléfonos de los alrededores se conecten a ellos y trasmitan datos y contenido de las comunicaciones”[27].

Aunque debido a la falta de transparencia y rendición de cuentas del Estado es imposible saber con exactitud qué tipos de vigilancia han realizado los órganos de inteligencia, qué tecnologías han usado y la identidad de todos sus objetivos, no se puede negar que la vigilancia ilegal de la CCAJAR no desapareció junto con el DAS. Desde 2013, los miembros de la CCAJAR han notado indicios de vigilancia al hablar por teléfono, al usar la computadora o en público. Los relatos de las autoridades colombianas y de los medios de comunicación confirman que los órganos de inteligencia siguen vigilando a miembros de la CCAJAR. El 18 de diciembre de 2019, una comisión de la Sala de Instrucción de la Corte Suprema de Justicia y policías judiciales de la Dirección de Investigaciones Especiales de la Procuraduría General allanaron el Batallón de Ciberinteligencia del Ejército[28]. Aunque los militares trataron de obstaculizar la inspección y ocultar pruebas[29], las autoridades judiciales incautaron programas informáticos y herramientas de vigilancia presuntamente utilizadas por las unidades de inteligencia militar para la vigilancia ilegal[30]. En los meses que siguieron al allanamiento, los medios de comunicación publicaron pruebas de que varias unidades de inteligencia militar habían llevado a cabo actividades de vigilancia ilegal para crear perfiles de periodistas, líderes sociales, políticos de la oposición, jueces y defensores de derechos humanos, entre ellos miembros de la CCAJAR[31]. Según el Relator Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (CIDH), “las tareas de vigilancia incluyeron la interceptación ilegal de comunicaciones, y un seguimiento a través de ‘StingRay’ [y programas maliciosos]”[32]. Estas revelaciones llevaron a la renuncia del general Nicasio Martínez, Comandante del Ejército Nacional, así como de otros altos oficiales, y el presidente Iván Duque ordenó al Ministro de Defensa “adelantar una rigurosa investigación de labores inteligencia de los últimos 10 años”[33]. El Relator Especial de la CIDH para la Libertad de Expresión ha expresado preocupación porque estas investigaciones penales “no han avanzado de manera significativa”[34].

2. El sistema de vigilancia de las comunicaciones de Colombia tiene implicaciones de gran alcance para una amplia gama de derechos humanos protegidos por la Convención Americana

---

[27] PRIVACY INTERNATIONAL, DEMANDA Y OFERTA: LA INDUSTRIA DE LA VIGILANCIA AL DESCUBIERTO 36 (2015), https://privacyinternational.org/sites/default/files/2017-12/DemandSupply_Espanol.pdf.

[28] CIDH, *Informe anual de la Relatoría Especial para la Libertad de Expresión*, párr. 407, OEA/Ser.L/V/II Doc. 28 (30 de marzo de 2021), http://www.oas.org/es/cidh/docs/anual/2020/capitulos/rele.PDF [en adelante “Informe de 2021 del Relator Especial de la CIDH para la Libertad de Expresión”].

[29] *“¡Tapen, tapen, tapen!”: así fue el allanamiento de la Corte Suprema a una instalación del Ejército*, SEMANA (13 de enero de 2020), https://www.semana.com/nacion/multimedia/nuevas-chuzadas-del-ejercito-en-colombia/647868/.

[30] Informe de 2021 del Relator Especial de la CIDH para la Libertad de Expresión, *supra,* nota 28, párr. 408 (donde se cita un informe de la Procuraduría sobre el allanamiento, en el cual se señala que el Batallón de Ciberinteligencia del Ejército “cuenta con la capacidad para acceder a cuentas de correo electrónico” e “intervenir comunicaciones”).

[31] *Las Carpetas Secretas*, SEMANA (5 de mayo de 2020), https://www.semana.com/nacion/articulo/espionaje-del-ejercito-nacional-las-carpetas-secretas-investigacion-semana/667616/; *Chuzadas sin Cuartel*, SEMANA (1 de enero de 2020), https://www.semana.com/nacion/articulo/chuzadas-por-que-se-retiro-el-general-nicacio-martinez-del-ejercito/647810/.

[32] Informe de 2021 del Relator Especial de la CIDH para la Libertad de Expresión, *supra,* nota 28, párr. 405.

[33] *Id.*, párr. 409.

[34] *Id.*, párr. 410.

El concepto jurídico del derecho a la privacidad surgió a raíz de las innovaciones tecnológicas del siglo XIX, entre ellas la invención de la fotografía y el advenimiento de los medios de comunicación masiva[35]. En 2013, con las revelaciones de Edward Snowden relativas a las actividades de vigilancia generalizada y mundial realizadas por los gobiernos, salió a plena luz el impacto de las técnicas de vigilancia estatal en la privacidad y en otros derechos humanos. Tras las revelaciones de Snowden, el derecho interno no ha logrado mantenerse a la par de los constantes adelantos tecnológicos que ofrecen a los Estados "una capacidad sin precedentes de caracterizar y someter a estrecho seguimiento, mediante métodos nuevos, el comportamiento de las personas"[36]. Con la disponibilidad de "un gran volumen de datos de transacciones de personas y acerca de estas"[37], los Estados "han ampliado sus atribuciones para llevar a cabo vigilancias, reduciendo las restricciones y aumentando las justificaciones de dicha vigilancia"[38]. Los órganos internacionales y regionales de derechos humanos han observado que los marcos jurídicos internos proporcionan a las personas "una protección limitada contra la vigilancia excesiva"[39].

Las actividades de inteligencia tienen enormes implicaciones para diversos derechos. En la era digital, el derecho a la privacidad se ha convertido en una "condición previa necesaria para la protección de valores fundamentales como la libertad, la dignidad, la igualdad y el derecho a no ser objeto de intrusión por parte de los Gobiernos, [...] un ingrediente fundamental para las sociedades democráticas"[40] y la puerta de entrada para la protección de otros derechos[41]. Por consiguiente, esta Corte debería determinar el impacto de la vigilancia estatal de los miembros de la CCAJAR y sus familiares en su derecho a la privacidad y en el goce de otros derechos humanos amparados por la Convención Americana, entre ellos el derecho a la vida y a la integridad personal, el acceso a la información y la libertad de expresión, de asociación y de circulación.

---

[35] Samuel D. Warren y Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890) (donde, en una de las primeras referencias al derecho a la privacidad, los autores afirman que las fotografías instantáneas y los periódicos han invadido los recintos sagrados de la vida privada y doméstica, y numerosos dispositivos mecánicos amenazan con convertir en realidad la predicción de que "lo que habéis susurrado en las habitaciones interiores, será proclamado desde las azoteas").

[36] Consejo de Derechos Humanos, *Informe del Relator Especial sobre el derecho a la privacidad*, párr. 33, U.N. Doc. A/HRC/40/63 (16 de octubre de 2019) [en adelante "Informe de 2019 del Relator Especial sobre el derecho a la privacidad"].

[37] Informe de 2013 del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión*, supra,* nota 9, párr. 15.

[38] *Id.*, párr. 16.

[39] Comité de Derechos Humanos, *Observaciones finales sobre el cuarto informe periódico de los Estados Unidos de América*, párr. 22, U.N. Doc. CCPR/C/USA/CO/4 (23 de abril de 2014) [en adelante *Observaciones finales del Comité de Derechos Humanos sobre Estados Unidos*] (donde se expresa preocupación acerca de la recolección de metadatos de comunicaciones en grandes cantidades por órganos de inteligencia del Estado, el secreto de los sistemas de supervisión y la falta de acceso de las personas afectadas a recursos efectivos). Véase también Tribunal Europeo de Derechos Humanos (TEDH), Roman Zakharov v. Russia, App. No. 47143/06 (4 de diciembre de 2015), https://hudoc.echr.coe.int/fre; Consejo de Derechos Humanos, *Informe del Relator Especial sobre el derecho a la privacidad*, párr. 15, U.N. Doc. A/HRC/34/60 (6 de septiembre de 2017) [en adelante "Informe de 2017 del Relator Especial sobre el derecho a la privacidad"] (donde se señala que, tras las revelaciones de Snowden, los Estados "aprobaron nuevas leyes sobre [vigilancia estatal] que solo incluyen, si acaso, leves mejoras en ámbitos limitados. En general, esas leyes han sido redactadas y sometidas a un apresurado proceso legislativo para legitimar prácticas que nunca deberían haberse aplicado").

[40] Informe de 2019 del Relator Especial sobre el derecho a la privacidad, *supra,* nota 36, párr. 51.

[41] Consejo de Derechos Humanos, *Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión*, párr. 16, U.N. Doc. A/HRC/29/32 (22 de mayo de 2015) [en adelante "Informe de 2015 del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión"].

Al evaluar la afectación de esos derechos, esta Corte debería tener en cuenta que el objetivo de la vigilancia de las comunicaciones llevada a cabo por Colombia no era proteger la seguridad nacional o el orden público, sino disuadir e impedir la labor de defensa de los derechos humanos. El derecho a defender los derechos humanos está amparado por diversos instrumentos y principios internacionales[42]. Esta Corte ha afirmado la importancia del trabajo en el ámbito de los derechos humanos, que es "fundamental para el fortalecimiento de la democracia y el Estado de Derecho"[43], y ha señalado que los Estados deben tomar ciertas medidas para proteger la labor de defensa de los derechos humanos y "facilitar los medios necesarios para que los defensores de derechos humanos realicen libremente sus actividades; protegerlos cuando son objeto de amenazas [...]; abstenerse de imponer obstáculos que dificulten la realización de su labor..."[44]. Colombia no ha cumplido estas obligaciones; en cambio, ha usado la vigilancia de las comunicaciones para atacar, amenazar, desacreditar, intimidar y silenciar a defensores de derechos humanos.

a. La vigilancia de las comunicaciones vulnera el derecho a la privacidad

El derecho a la privacidad es un derecho fundamental y universal amparado por el derecho internacional y la legislación interna[45]. El Pacto Internacional de Derechos Civiles y Políticos, el primer tratado internacional en el que se codificó este derecho en el derecho internacional de los derechos humanos, dispone que los Estados Partes se abstengan de someter a las personas a "injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación"[46]. Otros tratados internacionales de derechos humanos contienen disposiciones similares para proteger la privacidad de los niños[47], los trabajadores migrantes[48] y las personas con discapacidad[49]. También hay tratados

---

[42] Véase, por ejemplo, Asamblea General de las Naciones Unidas, resolución 53/144, *Declaración sobre el derecho y el deber de los individuos, los grupos y las instituciones de promover y proteger los derechos humanos y las libertades fundamentales universalmente reconocidos*, U.N. Doc.A/RES/53/144 (8 de marzo de 1999); Asamblea General de la Organización de los Estados Americanos (OEA), resolución AG/RES. 1671 (XXIX-O/99), *Defensores de los derechos humanos en las Américas: apoyo a las tareas que desarrollan las personas, grupos y organizaciones de la sociedad civil para la promoción y protección de los derechos humanos en las Américas* (7 de junio de 1999); Asamblea General de la OEA, resolución AG/RES 2517 (XXXIX-O/09), *Defensoras y defensores de los derechos humanos en las Américas: apoyo a las tareas que desarrollan las personas, grupos y organizaciones de la sociedad civil para la promoción y protección de los derechos humanos en las Américas* (4 de junio de 2009).

[43] Corte IDH, Caso Valle Jaramillo y otros vs. Colombia, Sentencia de 27 de noviembre de 2008 (Fondo, Reparaciones y Costas), serie C, No. 192, párr. 87 (27 de noviembre de 2008).

[44] Corte IDH, Caso Escher y Otros vs. Brasil, Sentencia de 6 de julio de 2009 (Excepciones Preliminares, Fondo, Reparaciones y Costas), serie C, No. 200, párr. 172.

[45] ACNUDH, *El derecho a la privacidad en la era digital. Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos*, párrs. 12 y 13, U.N. Doc. A/HRC/27/37 (30 de junio de 2014) [en adelante "Informe de 2014 del Alto Comisionado para los Derechos Humanos"].

[46] Pacto Internacional de Derechos Civiles y Políticos, art. 17, *abierto a la firma* el 16 de diciembre de 1966, 999 U.N.T.S.171. Véase también Declaración Universal de Derechos Humanos, art. 12, resolución de la Asamblea General 217 (III) A, U.N. Doc. A/810 (10 de diciembre de 1948).

[47] Convención sobre los Derechos del Niño, art. 16, *abierta a la firma* el 20 de noviembre de 1989, 1577 U.N.T.S. 3.

[48] Convención Internacional sobre la Protección de los Derechos de Todos los Trabajadores Migratorios y de sus Familiares, art. 14, *abierta a la firma* el 18 de diciembre de 1990, 2220 U.N.T.S. 3.

[49] Convención sobre los Derechos de las Personas con Discapacidad, anexo 1, art. 22, *abierta a la firma* el 13 de diciembre de 2005, 2515 U.N.T.S. 3.

regionales que prohíben la injerencia arbitraria y abusiva en la "vida privada, en la de su familia, en su domicilio o en su correspondencia"[50].

En la era digital, los órganos de derechos humanos entienden que el derecho a la privacidad se extiende a la privacidad de la información, "que abarca la información que existe o puede obtenerse acerca de una persona y de su vida y las decisiones basadas en esa información"[51]. Para proteger la privacidad de la información, la esfera privada, donde la persona presuntamente "debe tener una esfera de desarrollo autónomo, interacción y libertad"[52], abarca por necesidad no solo "los espacios privados, aislados, como el domicilio de una persona, sino que se extiende a los espacios públicos y a la información de acceso público"[53]. Por consiguiente, la protección de la privacidad se extiende no solo a "la información sustantiva contenida en las comunicaciones", sino también a los metadatos, que pueden "dar una mejor idea del comportamiento, las relaciones sociales, las preferencias privadas y la identidad de una persona que la información obtenida accediendo al contenido de una comunicación privada"[54].

De acuerdo con la Convención Americana, el derecho a la privacidad es un derecho relativo que puede restringirse solo "de una manera cuidadosamente delimitada"[55]. Las injerencias en este derecho son permisibles solo si no son ilícitas ni arbitrarias[56]. En el caso Escher contra Brasil, la Corte Interamericana reconoció el "riesgo intrínseco de abuso" de un sistema de vigilancia[57]. Según expertos internacionales, la mera existencia de una vigilancia

---

[50] OEA, Convención Americana sobre Derechos Humanos, art. 11, *abierta a la firma* el 22 de noviembre de 1969, O.A.S.T.S. No. 36; 1144 U.N.T.S. 123. En el Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales se especifica que la injerencia de la autoridad pública en el ejercicio del derecho al respeto a la vida privada y familiar debe estar prevista por la ley y constituir "una medida que, en una sociedad democrática, sea necesaria", ETS 5, art. 8 (1953) [en adelante "el Convenio Europeo"].

[51] Consejo de Derechos Humanos, *El derecho a la privacidad en la era digital. Informe del Alto Comisionado de las Naciones Unidas para los Derechos Humanos*, párr. 5, U.N. Doc. A/HRC/39/29 (3 de agosto de 2018) [en adelante "Informe de 2018 del Alto Comisionado para los Derechos Humanos"]. Véase también Informe de 2013 del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión*, supra,* nota 9, párr. 81 (donde se señala que la interceptación y la retención de datos sobre comunicaciones privadas infringe el derecho a la privacidad).

[52] Informe de 2018 del Alto Comisionado para los Derechos Humanos, *supra,* nota 51, párr. 5.

[53] *Id.*, párr. 6 (donde se cita el Comité de Derechos Humanos, *Observaciones finales sobre el séptimo informe periódico de Colombia*, párr. 32, U.N. Doc. CCCPR/C/COL/CO/7 (17 de noviembre de 2016) [en adelante *Observaciones finales del Comité de Derechos Humanos sobre Colombia (2016)*].

[54] Informe de 2018 del Alto Comisionado para los Derechos Humanos, *supra,* nota 51, párr. 6 (donde se cita el Informe de 2014 del Alto Comisionado para los Derechos Humanos, *supra,* nota 45, párr. 19). Véase Corte IDH, Caso Escher y otros vs. Brasil, serie C, No. 200, *supra,* nota 44, párr. 114 (donde se dispone que la protección de la vida privada se aplica a "cualquier otro elemento del proceso comunicativo mismo, por ejemplo, el destino de las llamadas que salen o el origen de las que ingresan, la identidad de los interlocutores, la frecuencia, hora y duración de las llamadas"); CIDH, *Estándares para una Internet Libre, Abierta e Incluyente*, párr. 189, OEA/Ser.L/V/II CIDH/RELE/INF.17/17 (15 de marzo de 2017) [en adelante *Estándares para Internet del Relator Especial de la CIDH para la Libertad de Expresión*] (donde se explica que los metadatos, "al igual que los datos relativos a las comunicaciones telefónicas, protegidos por la jurisprudencia del sistema interamericano, son distintos del contenido pero son altamente reveladores de relaciones personales, hábitos y costumbres, gustos, estilos y formas de vida, etc."); *id.*, párr. 213 (donde se señala que "[l]os estándares desarrollados tanto en el sistema interamericano como en el europeo apuntan a la protección no solo del contenido de las comunicaciones sino también a los datos respecto de esas comunicaciones, en el caso de internet").

[55] Informe de 2019 del Relator Especial sobre el derecho a la privacidad, *supra,* nota 36, párr. 11.

[56] *Id.*

[57] Corte IDH, Caso Escher y otros vs. Brasil, serie C, No. 200, *supra,* nota 44, párr. 118. Véase también Comité de Derechos Humanos, *Observación general No. 16: artículo 17 (derecho a la intimidad),* en *Recopilación de las observaciones generales y recomendaciones generales adoptadas por órganos de derechos humanos creados en virtud de tratados*, párrs. 3 y 4, U.N. Doc. HRI/GEN/Rev.9 (8 de abril de 1988).

secreta constituye una intrusión en el derecho a la privacidad[58] y una intensificación de la amenaza para una verdadera autonomía personal[59].

Aunque con la tecnología moderna es mucho más fácil para los Estados "conocer nuestra manera de actuar" y "limitar nuestra libertad para comportarnos como queramos"[60], los Estados no han adoptado "normas detalladas, procedimientos prácticos y mecanismos de supervisión adecuados que garanticen un control independiente, fiable y eficiente de las actividades de vigilancia, tanto a nivel nacional como internacional"[61]. Este entorno regulatorio ineficaz ha suscitado el interés de la comunidad internacional. Desde 2014, el Comité de Derechos Humanos de las Naciones Unidas ha expresado preocupación por la limitación arbitraria o ilegal de la privacidad en casi todas sus observaciones finales y en sus evaluaciones de las medidas tomadas por los países para cumplir las obligaciones asumidas en virtud del Pacto Internacional de Derechos Civiles y Políticos[62]. En sus observaciones finales sobre Colombia, por ejemplo, el Comité exhortó a los Estados a "[t]omar medidas eficaces para evitar que se realicen actividades ilegales de vigilancia" y "[a]doptar las medidas necesarias para garantizar que toda injerencia en el derecho a la vida privada, incluyendo aquellas que pudieran tener lugar en el marco del monitoreo del espectro electromagnético, cumpla con los principios de legalidad, necesidad y proporcionalidad"[63].

La jurisprudencia interamericana ha efectuado una importante contribución al desarrollo del derecho a la privacidad[64]. No obstante, excepto en el caso Escher contra Brasil, las sentencias de esta Corte se han centrado en intrusiones físicas en el derecho a la privacidad y, por lo tanto, no han abordado las implicaciones de la vigilancia tecnológica en los derechos humanos amparados por la Convención Americana y en su protección en este contexto. Este caso ofrece una oportunidad para que la Corte amplíe y aclare normas relacionadas con la injerencia en el derecho a la privacidad resultante de la vigilancia digital de las comunicaciones.

b. *La vigilancia de las comunicaciones vulnera los derechos a la vida y a la integridad personal*

En la Convención Americana se consagran los derechos a la vida y a la integridad personal[65]. Esta Corte ha afirmado también que "un Estado tiene la obligación de adoptar todas

---

58 Informe de 2018 del Alto Comisionado para los Derechos Humanos, *supra,* nota 51, párr. 7 (donde se cita TEDH, Roman Zakharov, App. No. 47143/06, *supra,* nota 39).

59 Informe de 2019 del Relator Especial sobre el derecho a la privacidad, *supra,* nota 36, párr. 10 (donde se señala que "la vulneración de la privacidad se enmarca en un sistema que pone en riesgo otras libertades. Y aunque con frecuencia estas vulneraciones las cometen agentes estatales con el objetivo de hacerse con el poder y conservarlo, a veces los responsables son instancias no estatales, como personas y empresas, que desean seguir ejerciendo control sobre otras personas").

60 *Id.*, párr. 8 (donde se cita a PAUL SIEGHART, PRIVACY AND COMPUTERS 24 [1976]).

61 Consejo de Derechos Humanos, *Informe del Relator Especial sobre el derecho a la privacidad*, párr. 53, U.N. Doc. A/HRC/37/62 (25 de octubre de 2018) [en adelante "Informe de 2018 del Relator Especial sobre el derecho a la privacidad"].

62 Véase PRIVACY INTERNATIONAL, GUIDE TO INTERNATIONAL LAW AND SURVEILLANCE 3.0 272-74 (2021), https://privacyinternational.org/report/4780/pis-guide-international-law-and-surveillance.

63 Véase *Observaciones finales del Comité de Derechos Humanos sobre Colombia (2016)*, *supra,* nota 53, párr. 33. Véase también *Observaciones finales del Comité de Derechos Humanos sobre Colombia (2010)*, *supra,* nota 5, párrs.16 y 17 (donde se toma nota de denuncias de vigilancia ilegal por órganos de inteligencia y se exhorta a Colombia a "crear sólidos sistemas de control y supervisión sobre los organismos de inteligencia").

64 Véase, por ejemplo, Corte IDH, Caso Escher y otros vs. Brasil, serie C, No. 200, *supra,* nota 44; Corte IDH, Caso Kimel vs. Argentina, Sentencia de 2 de mayo de 2008 (Fondo, Reparaciones y Costas), serie C, No. 177.

65 Convención Americana sobre Derechos Humanos, *supra,* nota 50, arts. 4 y 5.

las medidas necesarias y razonables para garantizar el derecho a la vida, libertad personal e integridad personal" de los defensores de derechos humanos[66]. Con ese fin, la Corte Interamericana ha dispuesto que los Estados velen para que los defensores de derechos humanos puedan realizar libremente sus actividades, que los protejan cuando sean objeto de amenazas y ataques y que investiguen eficazmente las violaciones cometidas en su contra[67].

Los órganos y expertos internacionales han reconocido que la vigilancia de las comunicaciones puede poner en peligro la vida y la seguridad[68]. El Relator Especial de las Naciones Unidas sobre la promoción y protección del derecho a la libertad de opinión y de expresión ha observado que "[l]os marcos jurídicos nacionales inadecuados propician la vulneración ilícita" de los derechos humanos por los órganos de inteligencia[69]. A su vez, "[l]a vigilancia de personas concretas —a menudo periodistas, activistas, personalidades de la oposición, críticos y otras personas que ejercían su derecho a la libertad de expresión— ha conducido en ocasiones a la detención arbitraria, a veces a la tortura y tal vez a ejecuciones extrajudiciales"[70].

En este caso, la Comisión Interamericana de Derechos Humanos ("la Comisión Interamericana") y los representantes de las víctimas argumentan que los órganos de inteligencia de Colombia usaron la vigilancia de las comunicaciones para acosar, intimidar y atacar a miembros de la CCAJAR y sus familiares[71]. Específicamente, al llevar este caso ante la Corte, la Comisión Interamericana concluyó que las operaciones de inteligencia "acrecientan el riesgo en el que [los miembros de la CCAJAR] desarrollan sus actividades" y generan la responsabilidad del Estado "por las amenazas, hostigamientos y actos de violencia en contra de los miembros" de la CCAJAR[72].

c. La vigilancia de las comunicaciones vulnera el derecho a la libertad de pensamiento y de expresión

La Corte Interamericana ha conferido amplia protección al derecho a la libertad de pensamiento y de expresión establecido en el artículo 13 de la Convención Americana, que abarca no solo el derecho a expresar ideas, sino también el derecho y la libertad de buscar,

---

66 Corte IDH, Caso Valle Jaramillo y otros vs. Colombia, serie C, No. 192, *supra,* nota 43, párr. 90.

67 *Id.*, párr. 91 (donde se cita Corte IDH, Resolución de la Corte Interamericana de Derechos Humanos de 9 de febrero de 2006, Medidas provisionales respecto de la República Bolivariana de Venezuela, Caso del Internado Judicial de Monagas ["La Pica"], párr. 14, https://www.corteidh.or.cr/docs/medidas/lapica_se_02.pdf; Corte IDH, Caso Nogueira de Carvalho y otro vs. Brasil, Sentencia de 28 de noviembre de 2006 [Excepciones Preliminares y Fondo], serie C, No. 161, párr. 77, y Corte IDH, Resolución de la Corte Interamericana de Derechos humanos de 30 de septiembre de 2006, Solicitud de medidas provisionales presentada por la Comisión Interamericana de Derechos Humanos respecto del Brasil a favor de las personas privadas de libertad en la Penitenciaría "Dr. Sebastião Martins Silveira" en Araraquara, São Paulo, Brasil, párr. 24, https://www.corteidh.or.cr/docs/medidas/araraquara_se_03.pdf).

68 Informe de 2018 del Relator Especial sobre el derecho a la privacidad, *supra,* nota 61, párr. 13.

69 Informe de 2013 del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, *supra,* nota 9, párr. 3.

70 Consejo de Derechos Humanos, *La vigilancia y los derechos humanos. Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión*, párr. 1, U.N. Doc. A/HRC/41/35 (28 de mayo de 2019) [en adelante "Informe de 2019 del Relator Especial sobre la libertad de opinión y de expresión"].

71 Véase, en general, CIDH, Informe No. 57/19, *supra,* nota 3.

72 *Id.*, párr. 296.

recibir y difundir información[73].Tres aspectos del derecho a la libertad de expresión son particularmente pertinentes para este caso debido a la índole política de la expresión que fue objeto de vigilancia y a las medidas tomadas por Colombia para desalentar e impedir la labor de defensa de los derechos humanos por medio de la vigilancia de las comunicaciones.

En primer lugar, la importancia de la libertad de expresión es uno de los principios fundamentales de la democracia y los derechos humanos[74]. El Relator Especial de las Naciones Unidas sobre la promoción y protección del derecho a la libertad de opinión y de expresión ha recalcado las graves implicaciones de la vigilancia de las comunicaciones para las sociedades democráticas, que "debe considerarse un acto sumamente perturbador que podría suponer una injerencia en los derechos a la libertad de expresión y la intimidad, y que atenta contra los fundamentos de una sociedad democrática"[75].

Segundo, los órganos internacionales y los tribunales han atribuido gran importancia a la "expresión sin inhibiciones"[76] y han expresado preocupación por el efecto corrosivo de la vigilancia en el debate público[77]. La vigilancia tiene un efecto intimidatorio en las personas porque "instala el temor y la inhibición como parte de la cultura política y las obliga a tomar precauciones para comunicarse entre ellas"[78]. Al debilitar la libertad de expresión, la vigilancia degrada el debate público en una sociedad democrática, especialmente cuando afecta a figuras de las esferas pública y política.

Las tecnologías digitales ofrecen a los Estados la capacidad sin precedentes para realizar actividades de vigilancia invasiva, tanto específica como masiva, de bajo costo, en secreto y de duración ilimitada[79]. El Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión ha señalado lo siguiente:

> ... las personas conservan sus opiniones en formato digital, al almacenar sus opiniones y su historial de búsqueda y de navegación, por ejemplo, en discos duros, en la nube y en archivos de correo electrónico que las autoridades privadas y públicas con frecuencia retienen por períodos largos o incluso indefinidos.

---

[73] Véase Corte IDH, Caso Herrera Ulloa vs. Costa Rica, Sentencia de 2 de julio de 2004 (Excepciones Preliminares, Fondo, Reparaciones y Costas), serie C, No. 107, párr. 108.

[74] El Tribunal Europeo de Derechos Humanos ha afirmado en reiteradas ocasiones la importancia de la libertad de expresión, y ha señalado que este derecho es uno de los fundamentos esenciales de una sociedad democrática y una de las condiciones básicas para su progreso y para la realización de cada persona. TEDH, Sürek v. Turkey (No. 3), App. Nos. 23927/94 and 24277/94, párr. 57 (1999), https://hudoc.echr.coe.int/fre?i=001-58278.

[75] Informe de 2013 del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, *supra,* nota 9, párr. 81.

[76] Comité de Derechos Humanos, *Observación general Nº 34. Artículo 19: Libertad de opinión y libertad de expresión*, párr. 34, U.N. Doc. CCPR/C/GC/34 (11 de septiembre de 2011).

[77] CIDH, Comunicado Conjunto. Relator Especial de las Naciones Unidas (ONU) para la Protección y Promoción del Derecho a la Libertad de Opinión y de Expresión, Relatora Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la OEA, *Declaración conjunta sobre programas de vigilancia y su impacto en la libertad de expresión*, párr. 5 (21 de junio de 2013), https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=927&lID=2 [en adelante *Declaración conjunta sobre la vigilancia*].

[78] CIDH, *Libertad de expresión e Internet*, párr. 150, OEA/Ser.L/V/II. CIDH/RELE/INF. 11/13 (2013) [en adelante "Informe de 2013 de la Relatora Especial de la CIDH para la Libertad de Expresión"].

[79] Informe de 2013 del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, *supra,* nota 9, párr. 33 (donde se señala que "los adelantos tecnológicos determinan que la eficacia del Estado para llevar a cabo la vigilancia ya no se vea limitada en función de la escala o la duración. Los menores costos de la tecnología y el almacenamiento de datos han permitido eliminar los desincentivos financieros o prácticos de realizar la vigilancia. En consecuencia, ahora el Estado tiene mayor capacidad que nunca para emprender una vigilancia simultánea, invasiva, selectiva y de escala amplia").

> Asimismo, las organizaciones de la sociedad civil preparan y almacenan en formato digital memorandos, ponencias y publicaciones que entrañan forjarse y mantener opiniones. En otras palabras, mantener una opinión en la era digital no es un concepto abstracto que se limita a lo que pueda estar en nuestra mente. Con todo, hoy las opiniones en el espacio digital son objeto de ataques[80].

Asimismo, el Relator Especial ha expresado especial preocupación por la forma en que "[l]os sistemas de vigilancia, tanto específicos como masivos, pueden vulnerar el derecho de las personas a forjarse opiniones, porque el temor a que su actividad en línea, como las búsquedas y las páginas visitadas, se divulgue sin su consentimiento probablemente puede disuadirlas de acceder a información, en especial si la vigilancia produce resultados represivos"[81]. Análogamente, el Tribunal de Justicia de la Unión Europea ha observado el efecto de la retención de datos por los gobiernos "en el uso de los medios de comunicación electrónica y, en consecuencia, en el ejercicio por los usuarios de esos medios de su libertad de expresión"[82].

El Relator Especial de las Naciones Unidas sobre el derecho a la privacidad ha señalado que, para prevenir o mitigar el efecto intimidatorio de la vigilancia, "[e]s esencial que los derechos humanos fundamentales, en particular la privacidad, la libertad de expresión y el derecho a la información, sigan ocupando un lugar central en las evaluaciones de las medidas de todo tipo de vigilancia del Estado"[83]. El Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión ha insistido en la adopción de leyes nacionales para limitar la vigilancia estatal a las circunstancias más excepcionales y exclusivamente bajo la supervisión de una autoridad judicial independiente[84]. A pesar de la creciente capacidad tecnológica, los Estados no han regulado el uso de la vigilancia de las comunicaciones de una forma acorde con las obligaciones emanadas del derecho internacional y regional de los derechos humanos[85] ni han establecido controles democráticos para el uso, la adquisición y la exportación de herramientas de vigilancia privadas. Estos controles y principios de derechos humanos son incluso más pertinentes en vista del importante papel que desempeñan en casos de vigilancia específica cuando está en juego la expresión de interés público[86].

Tercero, el reconocimiento por esta Corte de que la libertad de expresión consiste en un derecho público de acceso a información que obra en poder del Estado debería ser un elemento fundamental de la evaluación del impacto de la vigilancia de las comunicaciones en las protecciones conferidas en el artículo 13[87]. Esta Corte ha indicado reiteradamente la necesidad de

---

[80] Informe de 2015 del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, *supra,* nota 41, párr. 20.

[81] *Id.*, párr. 21.

[82] Tribunal de Justicia de la Unión Europea (TJUE), Asuntos acumulados núms. C-203/15 y C-698/15, Tele2 Sverige AB v. Post-och telestyrelsen, Secretary of State for the Home Department v. Watson, ECLI:EU:C:2016:970, párr. 101 (21 de diciembre de 2016) [en adelante "TJUE, Asuntos acumulados C-203/15 y C-698/15, Tele2 v. Post-och"]. Véase también TEDH, Rotaru v. Romania, App. No. 28341/91, párr. 46 (4 de mayo de 2000), https://hudoc.echr.coe.int/eng?i=001-58586; Consejo de Derechos Humanos, *Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión*, párr. 56, U.N. Doc. A/HRC/32/38 (11 de mayo de 2016).

[83] Informe de 2017 del Relator Especial sobre el derecho a la privacidad, *supra,* nota 39, párr. 35.

[84] Consejo de Derechos Humanos, *Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Frank La Rue. Adición. Misión a la ex República Yugoslava de Macedonia*, párr. 92, U.N. Doc. A/HRC/26/30/Add.2 (1 de abril de 2014).

[85] Informe de 2013 de la Relatora Especial de la CIDH para la Libertad de Expresión*, supra,* nota 78, párrs. 153, 155, 164 y 166.

[86] Informe de 2019 del Relator Especial sobre la libertad de opinión y de expresión, *supra,* nota 70, párr. 46.

[87] Corte IDH, Caso Claude Reyes y otros vs. Chile, Sentencia de 19 de septiembre de 20006 (Fondo, Reparaciones y Costas), serie C, No. 151, párrs. 84 y 85. Véase también *id.*, párr. 77.

que las sociedades democráticas "se rijan por el principio de máxima divulgación, el cual establece la presunción de que toda información es accesible"[88]. Recae en el Estado la carga de probar que toda información retenida se encuadra en "un sistema restringido de excepciones" de acuerdo con lo dispuesto en el artículo 13[89]. El Estado tiene la obligación positiva de proporcionar la información solicitada o dar una respuesta que justifique la restricción. Asimismo, esta Corte ha determinado que "las autoridades estatales no se pueden amparar en mecanismos como el secreto de Estado o la confidencialidad de la información, o en razones de interés público o seguridad nacional, para dejar de aportar la información requerida"[90].

d. La vigilancia de las comunicaciones vulnera la libertad de asociación y de circulación

En el artículo 16 de la Convención Americana se establece el "derecho a asociarse libremente" y se prohíben las restricciones salvo que estén "previstas por la ley" y sean "necesarias en una sociedad democrática". Esta Corte ha reconocido que la libertad de asociación tiene "un alcance y un carácter especial", con una dimensión tanto individual como social[91]. La dimensión individual consiste en "el derecho y la libertad de asociarse libremente con otras personas, sin intervención de las autoridades públicas que limiten o entorpezcan el ejercicio del respectivo derecho"[92], en tanto que la dimensión social se caracteriza por "habilitar a las personas para [...] actuar colectivamente para la consecución de los más diversos fines, siempre y cuando éstos sean legítimos"[93].

Por consiguiente, esta Corte ha concluido que el Estado no puede intervenir con el propósito de limitar u obstruir el ejercicio de la libertad de asociación ni ejercer presión o interferir en la consecución de un objetivo lícito común[94]. Además, ha recalcado el importante papel de los defensores de derechos humanos en las sociedades democráticas con el objetivo de imponer al Estado la obligación positiva de crear las condiciones jurídicas y fácticas necesarias para asegurar que aquellos que exponen violaciones de los derechos humanos puedan llevar a cabo sus actividades libremente[95].

El Relator Especial sobre el derecho a la privacidad ha subrayado la relación fundamental entre el derecho a la privacidad, la libertad de asociación y la salud de las sociedades

---

[88] *Id*., párr. 92.
[89] *Id.*
[90] Corte IDH, Caso Gomes Lund y otros (*"Guerrilha do Araguaia"*) vs. Brasil, Sentencia de 24 de noviembre de 2010 (Excepciones Preliminares, Fondo, Reparaciones y Costas), serie C, No. 11.552, párr. 202. Véase también Corte Suprema de Justicia, Sentencia T-374/20, 1 de septiembre de 2020, párr. 4.4 (Colombia), https://www.corteconstitucional.gov.co/relatoria/2020/T-374-20.htm (donde se reconoce que la víctima tiene derechos en el proceso penal de conformidad con el debido proceso, como el acceso efectivo a la administración de justicia, el derecho a la verdad, el acceso a expedientes penales y el derecho a participar activamente en el proceso penal).
[91] Corte IDH, Caso Huilca Tecse vs. Perú, Sentencia de 3 de marzo de 2005 (Fondo, Reparaciones y Costas), serie C, No. 121, párr. 69.
[92] *Id.*
[93] Corte IDH, Caso Escher y otros vs. Brasil, serie C, No. 200, *supra,* nota 44, párr.169. Véase también Corte IDH, Caso Huilca Tecse vs. Perú, serie C, No. 121, *supra,* nota 91, párr. 71.
[94] Corte IDH, Caso Cantoral Huamaní y García Santa Cruz vs. Perú, Sentencia de 10 de julio de 2007 (Excepción Preliminar, Fondo, Reparaciones y Costas), serie C, No. 167, párr. 144.
[95] Corte IDH, Caso Yarce y otras vs. Colombia, Sentencia de 22 de noviembre de 2016 (Excepción Preliminar, Fondo, Reparaciones y Costas), serie C, No. 325, párr. 271. Véase también Corte IDH, Caso Valle Jaramillo y otros vs. Colombia, serie C, No. 192, *supra,* nota 43, párr. 91.

democráticas. En ese sentido, señaló que "[l]a pérdida de la privacidad puede hacer que las personas pierdan [...] la confianza en el gobierno y las instituciones establecidas para representar los intereses públicos, y opten por no participar en la sociedad, lo cual puede afectar negativamente a las democracias representativas y ponerlas en peligro"[96]. Esta Corte también ha reconocido el efecto corrosivo de la vigilancia estatal en la posibilidad de una acción colectiva que la Convención Americana procura garantizar. En el caso Escher contra Brasil, la Corte dictaminó que el Estado había creado un clima de temor que obstaculizaba "el libre y normal ejercicio del derecho de asociación" al interceptar, monitorear y divulgar ilegalmente conversaciones telefónicas de miembros de organizaciones de defensa de los derechos humanos[97].

A pesar de las peligrosas implicaciones de la vigilancia para la salud de las democracias y la protección de los defensores de derechos humanos y en contravención de las normas internacionales, los Estados suelen promulgar leyes demasiado amplias y vagas que no disponen que la vigilancia esté dirigida a personas específicas sobre la base de una sospecha razonable[98]. En violación de la libertad de asociación, "[a]lgunos Estados han aprovechado la tecnología para vigilar y entorpecer la labor de los defensores de los derechos humanos y los agentes de la sociedad civil. [...] Muchos hackean teléfonos y ordenadores, lanzan amenazas de muerte y violación, divulgan imágenes manipuladas, suspenden temporalmente las cuentas de sus víctimas, secuestran etiquetas, propagan teorías sobre conspiraciones, vierten acusaciones de traición y promueven sentimientos discriminatorios virulentos"[99]. Según el Relator Especial sobre los derechos a la libertad de reunión pacífica y de asociación, el objetivo de estas tácticas es "intimidar a los agentes de la sociedad civil, destruir su credibilidad y legitimidad [...]. Esos ataques minan la capacidad que tienen las organizaciones de la sociedad civil y los activistas de difundir o recibir información y comunicarse con los demás. Incentivan la autocensura y amenazan la seguridad y la integridad personales"[100].

Asimismo, la praxis de los derechos humanos requiere que sus defensores tengan libertad de circulación y puedan elegir su lugar de trabajo y de residencia[101]. En el artículo 22 de la Convención Americana se establece "[el] derecho de [...] toda persona que se halle legalmente en

---

[96] Informe de 2019 del Relator Especial sobre el derecho a la privacidad, *supra,* nota 36, párr. 100.

[97] Corte IDH, Caso Escher y otros vs. Brasil, serie C, No. 200, *supra,* nota 44, párrs. 178 a 180.

[98] Consejo de Derechos Humanos, *Informe del Relator Especial sobre los derechos a la libertad de reunión pacífica y de asociación sobre su misión de seguimiento al Reino Unido de Gran Bretaña e Irlanda del Norte*, párr. 71, U.N. Doc. A/HRC/35/28/Add.1 (8 de junio de 2017) (donde se expresa preocupación por la definición demasiado amplia de "extremismo interno", que llevó a la presunta persecución por la policía de manifestantes pacíficos por considerarlos "extremistas internos" y a su inclusión en las bases de datos de inteligencia). Véase también Consejo de Derechos Humanos, *Informe del Relator Especial sobre los derechos a la libertad de reunión pacífica y de asociación*, párr. 57, U.N. Doc. A/HRC/41/41 (17 de mayo de 2019) [en adelante "Informe de 2019 del Relator Especial sobre la libertad de reunión pacífica y de asociación"] (donde se señala que "[l]a vigilancia de los particulares que ejercen esos derechos suyos solo se puede llevar a cabo de manera específica, cuando haya una sospecha razonable de que están implicados en delitos penales graves o prevén implicarse en ellos y aplicando las normas más estrictas y los principios de necesidad y proporcionalidad, bajo supervisión judicial rigurosa"); Comité de Derechos Humanos, *Observación general núm. 37 (2020) relativa al derecho de reunión pacífica (artículo 21)*, párr. 61, U.N. Doc. CCPR/C/GC/37 (17 de septiembre de 2020) (donde se afirma que, en el contexto de reuniones pacíficas, la vigilancia estatal "no debe dar lugar a la supresión de derechos o tener un efecto disuasorio" y esas actividades "deben ajustarse estrictamente a las normas internacionales aplicables, especialmente sobre el derecho a la intimidad, y nunca pueden tener por objeto intimidar u hostigar a los participantes o los posibles participantes en las reuniones").

[99] Informe de 2019 del Relator Especial sobre la libertad de reunión pacífica y de asociación, *supra,* nota 98, párr. 43.

[100] *Id.*, párr. 44.

[101] CIDH, *Informe sobre la situación de las defensoras y defensores de los derechos humanos en las Américas*, OEA/Ser.L/V/II.124 Doc. 5 rev.1, párr. 101 (2006).

territorio de un Estado [...] a circular y a residir libremente dentro de él, y el derecho de ingresar, permanecer y salir del territorio del Estado sin interferencia ilegal"[102]. Para proporcionar asistencia letrada, en particular, los abogados necesitan mantener una relación y comunicación estrechas con las víctimas que representan. La Corte ha afirmado que "el derecho de circulación y de residencia puede ser vulnerado por restricciones de facto si el Estado no ha establecido las condiciones ni provisto los medios que permiten ejercerlo"[103]. En este caso, los miembros de la CCAJAR se vieron obligados a limitar sus actividades, a cambiar de domicilio y a exiliarse debido a los actos de violencia, las amenazas y el acoso que sufrieron como consecuencia de operaciones de inteligencia del Estado. La persecución impuso restricciones al movimiento que obstruyeron la libertad de los miembros de la CCAJAR para asociarse libremente con otras personas y llevar a cabo la labor colectiva de defensa de los derechos humanos.

Este caso ilustra los efectos insidiosos de la vigilancia en la libertad de asociación y de circulación. Durante décadas se proyectó sobre cada decisión de los miembros de la CCAJAR la sombra de la vigilancia, que limitó su autonomía personal y obstaculizó sus actividades de defensa de los derechos humanos.

e. La vigilancia de las comunicaciones pone en peligro los derechos de los niños

De acuerdo con el artículo 19 de la Convención Americana, "[t]odo niño tiene derecho a las medidas de protección que su condición de menor requieren por parte de su familia, de la sociedad y del Estado"[104]. Esta Corte ha afirmado reiteradamente que los niños "poseen los derechos que corresponden a todos los seres humanos" y "tienen además derechos especiales derivados de su condición, a los que corresponden deberes específicos de la familia, la sociedad y el Estado"[105]. En opinión de esta Corte, el artículo 19 impone una condición especial al Estado en calidad de garante de los derechos del niño[106]. Por consiguiente, la Corte entiende que el artículo 19 impone al Estado la obligación de tomar todas las medidas que sean necesarias para asegurar el goce efectivo de los derechos del niño, eliminando cualquier obstáculo y teniendo en cuenta las circunstancias y las dificultades particulares que enfrentan los niños en el goce de sus derechos[107]. Asimismo, esta Corte ha aplicado una norma más estricta para evaluar la conducta del Estado que vulnera la integridad física, mental o moral, porque los niños necesitan protección especial en vista de su grado de desarrollo[108].

---

[102] CIDH, Informe No. 57/19, *supra,* nota 3, párr. 329.

[103] Corte IDH, Caso Valle Jaramillo y otros vs. Colombia, serie C, No. 192, *supra,* nota 43, párr. 139.

[104] Convención Americana sobre Derechos Humanos, *supra,* nota 50, art. 19.

[105] Corte IDH, Opinión Consultiva OC-17/2002 de 28 de agosto de 2002, Condición Jurídica y Derechos Humanos del Niño, serie A. No. 17, párr. 54.

[106] Corte IDH, Caso de los Hermanos Gómez Paquiyauri vs. Perú, Sentencia de 8 de julio de 2004 (Fondo, Reparaciones y Costas), serie C, No. 110, párrs. 124, 163, 164 y 171.

[107] Corte IDH, Caso de los "Niños de la Calle" (Villagrán Morales y otros vs. Guatemala), Sentencia de 19 de noviembre de 1999 (Fondo), serie C, No. 63, párrs. 144 y 191; Corte IDH, Caso Chitay Nech y otros vs. Guatemala, Sentencia de 25 de mayo de 2010 (Excepciones Preliminares, Fondo, Reparaciones y Costas), serie C, No. 212, párr. 169; Corte IDH, Caso "Instituto de Reeducación del Menor" vs. Paraguay, Sentencia de 2 de septiembre de 2004 (Excepciones Preliminares, Fondo, Reparaciones y Costas), serie C, No. 112, párr.161.

[108] Corte IDH, Caso Furlan y familiares vs. Argentina, Sentencia de 31 de agosto de 2012 (Excepciones Preliminares, Fondo, Reparaciones y Costas), serie C, No. 246, párrs. 125 a 127. Con respecto al derecho del niño a la privacidad, la Corte Interamericana determinó que este derecho fue vulnerado cuando los menores que eran familiares de las víctimas fueron

Las violaciones de la privacidad de los niños tienen implicaciones de gran alcance para el goce de otros derechos. Según el Relator Especial sobre el derecho a la privacidad:

> Los derechos del niño son universales, indivisibles e interdependientes y están relacionados entre sí. El derecho del niño a la privacidad le permite acceder a otros derechos fundamentales para el desarrollo de la personalidad y la persona, como el derecho a la libertad de expresión y de asociación y el derecho a la salud, entre otros. La privacidad de los niños está relacionada con su integridad física y psíquica, su autonomía para tomar decisiones, su identidad personal, su privacidad en relación con la información y su privacidad desde el punto de vista físico y espacial *(citas omitidas)*[109].

Con respecto a la privacidad de la información, el Comité de los Derechos del Niño, de las Naciones Unidas, ha exhortado a los Estados a "adoptar todas las medidas apropiadas para velar por que la recopilación, el almacenamiento y el uso de datos personales delicados sean compatibles con las obligaciones contraídas en virtud del artículo 16 de la Convención"[110]. Más específicamente, el Comité de los Derechos del Niño ha recomendado que:

> Se adopten medidas eficaces para velar por que esa información no caiga en manos de personas no autorizadas por la ley para recibirla, elaborarla y emplearla [y que] [l]os niños y los padres bajo su jurisdicción tengan derecho a acceder a sus datos y a pedir la rectificación o eliminación de información cuando sea incorrecta o se haya compilado contra su voluntad o en contravención de las disposiciones de la Ley[111].

La vigilancia estatal tiene implicaciones diferentes para los menores. El Comité de los Derechos del Niño ha señalado que el derecho a la privacidad es "vital para la autonomía, la dignidad y la seguridad de los niños y para el ejercicio de sus derechos"[112] y que la vigilancia masiva tiene "consecuencias adversas para estos, cuyo efecto podría continuar en etapas posteriores de su vida"[113]. Las consecuencias de la vigilancia y la retención de datos obtenidos por este medio podrían persistir por décadas. La vigilancia específica ilegal o irregular podría tener consecuencias irreparables en el desarrollo individual de los menores, que son particularmente vulnerables a la estigmatización. Si se los tacha de "delincuentes" o "subversivos" como consecuencia de la vigilancia estatal ilegal y arbitraria, eso podría tener efectos profundos en su acceso a la educación, la atención de salud, el empleo y otros derechos. En vista de ello, el Comité de los Derechos del Niño ha reafirmado la obligación del Estado de "garantizar que los niños y sus padres o cuidadores puedan acceder fácilmente a los datos

---

sometidos "al odio, desprecio público, persecución y a la discriminación" después que el Estado de Perú trató erróneamente a las víctimas como terroristas. Corte IDH, Caso de los Hermanos Gómez Paquiyauri vs. Perú, serie C, No. 110*, supra,* nota 106, párrs. 182 y 253 (7).

[109] Consejo de Derechos Humanos, *La inteligencia artificial y la privacidad, así como la privacidad de los niños. Informe del Relator Especial sobre el derecho a la privacidad*, párr. 71, U.N. Doc. A/HRC/46/37 (21 de enero de 2021).

[110] Comité de los Derechos del Niño, *Observaciones finales del Comité de los Derechos del Niño: Francia*, párr. 51, U.N. Doc. CRC/FRA/CO/4 (22 de junio de 2009) [en adelante "Informe de 2009 del Comité de los Derechos del Niño"]. Véase también Comité de los Derechos del Niño, *Concluding Observations on the Second Periodic Report of Kuwait*, párr. 18, U.N. Doc. CRC/C/ KWT/CO/2 (29 de octubre de 2013) (donde se insta al Estado Parte a que elabore y aplique una política para proteger la privacidad de todos los menores inscritos en la base de datos nacional); Comité de los Derechos del Niño, *Observaciones finales. Reino Unido de Gran Bretaña e Irlanda del Norte*, párr. 37.a, U.N. Doc. CRC/C/GBR/CO/4 (20 de octubre de 2008) (donde se recomienda "que los niños estén protegidos contra toda injerencia arbitraria o ilícita en su vida privada, en particular adoptando una regulación más estricta de la protección de datos").

[111] Informe de 2009 del Comité de los Derechos del Niño, *supra,* nota 110, párr. 51.

[112] Comité de los Derechos del Niño, *Observación general núm. 25 (2021) relativa a los derechos de los niños en relación con el entorno digital*, párr. 67, U.N. Doc. CRC/C/GC/25 (2 de marzo de 2021) [en adelante *Observación general núm. 25 del Comité de los Derechos del Niño*].

[113] *Id.*, párr. 68.

almacenados, rectificar los que sean inexactos u obsoletos y eliminar los datos almacenados de forma ilegal o innecesaria por autoridades públicas, particulares u otras entidades, con sujeción a limitaciones razonables y legales"[114]. A fin de ejercer este derecho a examinar y rectificar los datos que obren en poder del Estado, es necesario tener conocimiento de su recopilación, monitoreo y almacenamiento. Por lo tanto, la existencia de recursos para casos de abuso y vigilancia específica ilegal de menores es muy pertinente en este contexto.

En el informe de fondo de la Comisión, se señala la realización de operaciones de inteligencia dirigidas a miembros de la CCAJAR y sus familiares, incluidos sus hijos[115]. Este caso ofrece a la Corte una oportunidad para formular disposiciones que protejan firmemente los derechos del niño de la injerencia de órganos de inteligencia. Con ese fin, esta Corte debería reconocer una presunción en contra de la vigilancia estatal de menores. Asimismo, debería imponer restricciones estrictas para que toda medida adoptada por el Estado que vulnere el derecho a la privacidad de un menor tenga en cuenta "el interés superior del niño" y los "derechos especiales" del niño señalados por las normas internacionales, en particular las protecciones establecidas por esta Corte[116]. Además de las salvaguardias dispuestas en el derecho internacional de los derechos humanos para la vigilancia estatal de toda persona, la vigilancia de menores debe estar acompañada de varias protecciones adicionales, entre ellas evaluaciones minuciosas de la excepcionalidad y la proporcionalidad, controles judiciales estrictos y más uniformes, y límites especiales para la retención de datos de menores.

B. COLOMBIA NO HA REGULADO DE MANERA ADECUADA LA VIGILANCIA DE LAS COMUNICACIONES POR ÓRGANOS DE INTELIGENCIA EN VIOLACIÓN A LOS DERECHOS PROTEGIDOS POR LA CONVENCIÓN AMERICANA

Durante décadas, Colombia ha usado herramientas de vigilancia invasiva para interceptar las comunicaciones privadas de miembros de la CCAJAR y sus familiares. Para responder a las críticas de la vigilancia de los defensores de derechos humanos, en 2013 Colombia promulgó la Ley de Inteligencia 1621 ("Ley de Inteligencia de 2013" o "Ley de Inteligencia")[117]. Durante la audiencia pública frente esta Corte, Colombia insiste en que esta ley "establece de manera clara y precisa las circunstancias concretas en que [las labores de inteligencia] pueden ser autorizadas para garantizar que toda actuación se ajuste a los principios de legalidad, proporcionalidad y necesidad" y que "dispone controles en varios niveles frente el desarrollo" de actividades de inteligencia[118].

---

[114] *Id.*, párr. 72.

[115] CIDH, Informe No. 57/19, *supra,* nota 3, párr. 177-179. Los órganos de las Naciones Unidas han expresado preocupación reiteradamente por el involucramiento de niños en labores de inteligencia. Véase *Observaciones finales del Comité de Derechos Humanos sobre Colombia (2016)*, *supra,* nota 53, párr. 41; Comité de los Derechos del Niño, *Observaciones finales sobre los informes periódicos cuarto y quinto combinados de Colombia*, párr. 65(e), U.N. Doc. CRC/C/COL/CO/4-5 (6 de marzo de 2015).

[116] Convención sobre los Derechos del Niño, *supra*, nota 47, arts. 3 y 16; Corte IDH, Opinión Consultiva OC-17/2002, *supra*, nota 105, párr. 54.

[117] CIDH, Informe No. 57/19, *supra,* nota 3, párr. 59.

[118] Audiencia Pública del Caso Miembros Corporación Colectivo de Abogados CAJAR vs. Colombia Parte 2, *supra,* nota 1, 8:32:28-8:32:49.

En la Ley de Inteligencia no se autoriza explícitamente a los órganos de inteligencia colombianos a interceptar comunicaciones privadas. De hecho, en las leyes colombianas no se prevé que cualquier autoridad esté facultada para interceptar comunicaciones con fines que no sean investigaciones penales. No obstante, los órganos de inteligencia de Colombia han llevado a cabo de manera sistemática actividades de inteligencia que no están previstas en la ley, han abusado de la vaguedad de las principales disposiciones de la Ley de Inteligencia relacionadas con el monitoreo del espectro electromagnético y se han aprovechado de la débil supervisión, en contravención de la Convención Americana. El Estado de Colombia no ha explicado la forma en que continuó la vigilancia ilegal de miembros de la CCAJAR tras la disolución del DAS, sino que simplemente se insiste en que la Ley de Inteligencia es adecuada.

Para examinar la afirmación del Gobierno de Colombia de que su marco jurídico actual es adecuado, esta Corte debería examinar las normas interamericanas e internacionales de derechos humanos que establecen requisitos mínimos para un marco regulatorio integral aplicable a los sistemas y las actividades estatales de vigilancia de las comunicaciones[119]. Aunque el derecho internacional de los derechos humanos dispone claras restricciones y limitaciones al uso de herramientas de vigilancia y a la injerencia en el derecho a la privacidad, los detalles relativos a los marcos que limitan la vigilancia de manera adecuada todavía están en evolución. Esta Corte ocupa una posición singular para desarollar normas en este campo. En los casos en que haya normas contradictorias o brechas en el derecho internacional, esta Corte debería examinar el contexto y las prácticas utilizadas en el país en cuestión a lo largo de su historia. Esta Corte debería tener en cuenta el historial preocupante de Colombia de uso de métodos de vigilancia abusivos y aplicar las normas de protección más estrictas que sea posible[120]. Un examen de la Ley de Inteligencia de Colombia, junto con las leyes y políticas en materia de retención de teledatos de las comunicaciones y acceso a los mismos, protección de los datos, transferencias de datos al exterior y acceso público a la información, muestra que Colombia no cumple sus obligaciones internacionales, poniendo en gran riesgo el trabajo y la vida de los defensores de derechos humanos y sus familiares. Las consecuencias de la vigilancia de defensores de derechos humanos, entre ellos miembros de la CCAJAR, sin ningún tipo de fiscalización, son profundamente amenazadoras para la democracia de Colombia y para las personas que trabajan en asuntos de interés público.

1. Esta Corte debe examinar la vigilancia que se lleva a cabo en Colombia a la luz de las normas internacionales de derechos humanos que confieren la mayor protección

a. Es necesario reglamentar la vigilancia de las comunicaciones por las autoridades de inteligencia a fin de que se ciña a las normas de legalidad,

[119] Esta Corte ha recurrido siempre a la jurisprudencia de otros órganos de derechos humanos para interpretar el alcance y el contenido del concepto de necesidad. Véase, por ejemplo, Corte IDH, Caso Herrera Ulloa vs. Costa Rica, serie C, No. 107, *supra,* nota 73, párrs. 121, 122, 125 y 126 (donde se tienen en cuenta las normas internacionales en materia de derechos humanos para establecer restricciones apropiadas a la libertad de expresión); Corte IDH, Caso de la "Masacre de Mapiripán" vs. Colombia, Sentencia de 15 de septiembre de 2005 (Fondo, Reparaciones y Costas), serie C, No. 134, párr. 153 (donde se tienen en cuenta las normas internacionales para establecer el alcance y el contenido de los derechos del niño).

[120] Véase, por ejemplo, TEDH, Ekimdzhiev v. Bulgaria, App. No. 70078/12, párr. 293 (11 de enero de 2022), https://hudoc.echr.coe.int/eng (donde se formula el razonamiento de que los tribunales deben examinar el funcionamiento real del régimen de vigilancia y la existencia o la ausencia de un abuso real al determinar si las leyes ofrecen garantías efectivas contra la vigilancia abusiva).

legitimidad, idoneidad, necesidad y proporcionalidad establecidas en la Convención Americana

De acuerdo con la Convención Americana, toda actividad del Estado que constituya una injerencia en los derechos amparados por la Convención debe ceñirse a los principios fundamentales de legalidad, legitimidad, idoneidad, proporcionalidad y necesidad[121], que esta Corte ha aplicado al determinar si la vigilancia estatal de las comunicaciones es compatible con las disposiciones de la Convención Americana[122]. Asimismo, el Tribunal Europeo de Derechos Humanos y el Comité de Derechos Humanos han reafirmado estos principios en reiteradas ocasiones al evaluar los marcos jurídicos que regulan las actividades de vigilancia estatal, incluidos los regímenes de vigilancia establecidos para velar por la seguridad nacional[123]. Esta Corte debe determinar si las actividades y las leyes de Colombia en el ámbito de la vigilancia se ciñen a estos principios.

Primero, de acuerdo con el principio de legalidad, toda injerencia en los derechos humanos causada por la vigilancia estatal debe ser accesible y previsible. Eso significa que las condiciones conforme a las cuales se autoriza una injerencia deben estar "claramente establecidas por ley", y la injerencia es permisible solo si se efectúa de conformidad a las leyes[124]. La injerencia debe estar "prevista" en la ley[125]. Si las autoridades llevan a cabo una actividad que no esté autorizada por ley o que esté explícitamente prohibida por ley, eso constituye una violación del principio de legalidad[126].

El principio de legalidad también exige, según esta Corte, que las leyes internas que autoricen la injerencia en derechos humanos amparados por la Convención sean precisas y claras, a fin de que se pueda prever cómo se aplicarán[127]. Esta Corte y el Tribunal Europeo de Derechos Humanos han afirmado que las "reglas claras y detalladas" son especialmente importantes en el contexto del sigilo que rodea a la vigilancia estatal, en el cual hay un mayor riesgo de que el Estado aplique las leyes de manera arbitraria y cometa abusos[128]. La claridad y

---

121 Convención Americana sobre Derechos Humanos, *supra,* nota 50, arts. 11.2, 13.2, 30 y 32.2.

122 Corte IDH, Caso Escher y otros vs. Brasil, serie C, No. 200, *supra,* nota 44, párr. 129; Corte IDH, Caso Tristán Donoso vs. Panamá, Sentencia de 27 de enero de 2009 (Excepciones Preliminares, Fondo, Reparaciones y Costas), serie C, No. 193, párr. 76.

123 TEDH, Big Brother Watch v. United Kingdom, App. No. 58170/13, párr. 332 (25 de mayo de 2021), https://hudoc.echr.coe.int/fre?i=001-210077; TEDH, Roman Zakharov, App. No. 47143/06, *supra,* nota 39, párr. 227 (donde se analiza la impugnación por un periodista de la interceptación de conversaciones telefónicas sin autorización judicial previa); Comité de Derechos Humanos, *Observaciones finales sobre el quinto informe periódico de Belarús*, párr. 44, U.N. Doc. CCPR/C/BLR/CO/5 (22 de noviembre de 2018) [en adelante *Observaciones finales del Comité de Derechos Humanos sobre Belarús*].

124 Corte IDH, Caso Escher y otros vs. Brasil, serie C, No. 200, *supra,* nota 44, párr. 130; Corte IDH, Caso Tristán Donoso vs. Panamá, serie C, No. 193, *supra,* nota 122, párr. 56.

125 *Id.*, párr. 76.

126 *Id.*, párr. 80 (donde se concluye que la divulgación a terceros de grabaciones de conversaciones telefónicas entre el abogado y su cliente infringió el principio de legalidad).

127 Corte IDH, Caso Escher y otros vs. Brasil, serie C, No. 200, *supra,* nota 44, párr. 118; Corte IDH, Caso Tristán Donoso vs. Panamá, serie C, No. 193, *supra,* nota 122, párr. 77; Corte IDH, Caso Kimel vs. Argentina, serie C, No. 177, *supra,* nota 64, párr. 63. Véase también Informe de 2013 de la Relatora Especial de la CIDH para la Libertad de Expresión, *supra,* nota 78, párr. 153.

128 Corte IDH, Caso Escher y otros vs. Brasil, serie C, No. 200, *supra,* nota 44, párr. 118. Véase también TEDH, Szabo v. Hungary, App. No. 37138/14, párr. 62 (12 de enero de 2016), https://hudoc.echr.coe.int/fre?i=001-160020.

la precisión son incluso más cruciales con el aumento de la sofisticación de la tecnología[129], razón por la cual la ley en cuestión debe ser del dominio público[130]. "Las normas y las interpretaciones secretas" no son compatibles con esta norma[131].

Para evaluar exhaustivamente la claridad y la precisión de las leyes colombianas en materia de vigilancia, esta Corte debería examinar la lista de requisitos mínimos establecidos en la jurisprudencia y las normas interamericanas. En 2009, esta Corte indicó varios elementos que deben establecerse en las leyes internas sobre vigilancia, como "las circunstancias en que dicha medida puede ser adoptada; las personas autorizadas a solicitarla, a ordenarla y a llevarla a cabo; el procedimiento a seguir, entre otros elementos"[132]. En 2013, el Relator Especial de la CIDH para la Libertad de Expresión y el Relator Especial de las Naciones Unidas sobre la libertad de opinión y de expresión se explayaron acerca de esta jurisprudencia y afirmaron que la normativa interna "deberá establecer límites respecto a la naturaleza, alcance y duración de este tipo de medidas, las razones para ordenarlas, las autoridades competentes para autorizar, ejecutar y supervisarlas y los mecanismos legales para su impugnación"[133].

El Tribunal Europeo de Derechos Humanos ha establecido requisitos mínimos para las leyes internas que regulan la vigilancia, que coinciden en parte con las normas establecidas por esta Corte. El Tribunal requiere que las leyes internas sobre vigilancia, incluso en el marco de la obtención de inteligencia con fines de seguridad nacional, describan de manera precisa 1) los motivos por los cuales se puede recurrir a la vigilancia secreta; 2) las personas que pueden ser vigiladas; 3) la duración de las medidas de vigilancia secreta; 4) los procedimientos para la autorización; 5) los procedimientos para el almacenamiento, el acceso, el examen y el uso de los datos obtenidos; 6) los procedimientos para la comunicación de datos de vigilancia a terceros; 7) los procedimientos para la destrucción de datos de vigilancia; 6) los mecanismos de supervisión; 8) la notificación, y 9) los recursos[134].

Además, en los casos como el presente en que las actividades de vigilancia estén dirigidas o puedan estar dirigidas a las comunicaciones de defensores de derechos humanos, entre ellos abogados, debería haber mayor protección. Esta Corte y el Tribunal Europeo de Derechos Humanos han reconocido la necesidad de "un mayor grado de protección" y la importancia de garantías procesales específicas para las comunicaciones amparadas por el secreto profesional, entre ellas las comunicaciones de abogados y periodistas[135]. En vista de la

---

129 Corte IDH, Caso Escher y otros vs. Brasil, serie C, No. 200, *supra,* nota 44, párr. 115; TEDH, Szabo, App. No. 37138/14, *supra,* nota 128, párr. 62.

130 Consejo de Derechos Humanos, resolución 48/4, preámbulo, U.N. Doc. A/HRC/RES/48/4 (7 de octubre de 2021).

131 Informe de 2014 del Alto Comisionado para los Derechos Humanos, *supra,* nota 45, párr. 29.

132 Corte IDH, Caso Escher y otros vs. Brasil, serie C, No. 200, *supra,* nota 44, párr. 131.

133 *Declaración conjunta sobre la vigilancia*, *supra,* nota 77, párr. 9.

134 TEDH, Ekimdzhiev, App. No. 70078/12, *supra,* nota 120, párrs. 294 a 355 (donde se examina el marco jurídico de la vigilancia secreta, incluso con fines de seguridad nacional); TEDH, Szabo, App. No. 37138/14, *supra,* nota 128, párrs. 55 a 57.

135 Corte IDH, Caso Tristán Donoso vs. Panamá, serie C, No. 193, *supra,* nota 122, párr. 75. Véase también TEDH, Ekimdzhiev, App. No. 70078/12, *supra,* nota 120, párr. 333 (donde se describe la necesidad de mayor protección con respecto a la interceptación de comunicaciones respecto de las cuales se tiene derecho a mantener reserva); TEDH, Sommer v. Germany, App. No. 73607/13, párr. 56 (27 de abril de 2017), https://hudoc.echr.coe.int/eng?i=001-173091 (donde se aborda la importancia de las salvaguardias procesales para la interceptación de comunicaciones entre los abogados y sus clientes en el contexto de las investigaciones penales); TEDH, Iordachi v. Moldova, App. No. 25198/02, párr. 50 (24 de septiembre de 2009), https://hudoc.echr.coe.int/fre?i=002-1661 (donde se señala la falta de normas claras con respecto a la forma en que las

índole de sus comunicaciones, se les debería aplicar esta mayor protección a todos los defensores de derechos humanos[136].

En segundo lugar, el principio de legitimidad requiere que las leyes que vulneren cualquiera de los derechos enumerados en la Convención Americana "se dictaren por razones de interés general y con el propósito para el cual han sido establecidas"[137]. En otras palabras, toda injerencia en los derechos humanos resultante de la vigilancia estatal debe "perseguir un fin legítimo"[138]. En la Convención Americana se enumeran varios fines que pueden ser legítimos, como la seguridad pública, la salud, la moral y el orden público, los derechos y las libertades de los demás, y la seguridad nacional[139]. Sin embargo, esta Corte ha señalado que no basta con invocar un fin legítimo para justificar una injerencia en los derechos amparados por la Convención Americana. Específicamente, esta Corte dictaminó que la invocación de la "seguridad nacional" para calificar de amenaza "a cualquiera que, real o presuntamente, respaldara la lucha para cambiar el orden establecido", incluidos los defensores de derechos humanos, vulnera los derechos y las libertades[140]. Esto es una maniobra que Colombia ha usado y sigue usando para disuadir e impedir la legítima labor de defensa de los derechos humanos realizadas por los miembros de la CCAJAR[141]. En vista de ello, el Relator Especial de la CIDH para la Libertad de Expresión y el Relator Especial de las Naciones Unidas sobre la libertad de opinión y de expresión han aconsejado un escrutinio riguroso: "Cuando se invoque la seguridad nacional como razón para vigilar la correspondencia y los datos personales, la ley debe

---

autoridades deben manejar las comunicaciones entre los abogados y sus clientes durante la vigilancia); TEDH, Sedletska v. Ukraine, App. No. 42634/18, párr. 62 (1 de abril de 2021) (donde se señala que el Tribunal ha señalado reiteradamente que las limitaciones de la confidencialidad de las fuentes periodísticas exigen el examen más riguroso posible).

136 Véase, por ejemplo, Consejo de Derechos Humanos, resolución 48/4, párr. 6.k, U.N. Doc. A/HRC/Res/48/4 (13 de octubre de 2021).

137 Convención Americana sobre Derechos Humanos, *supra,* nota 50, art. 30.

138 Corte IDH, Caso Escher y otros vs. Brasil, serie C, No. 200, *supra,* nota 44, párr. 129.

139 Convención Americana sobre Derechos Humanos, *supra,* nota 50, arts. 13.2 y 16.2. Véase también Convención Internacional sobre la Protección de los Derechos de Todos los Trabajadores Migratorios y de sus Familiares, art. 19.3, 18 de diciembre de 1990, 2220 U.N.T.S. 3; Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, art. 8.2, ETS No. 005 (1953).

140 Corte IDH, Caso Molina Theissen vs. Guatemala, Sentencia de 4 de mayo de 2004 (Fondo), serie C, No. 106, párr. 40.2. Véase también Corte IDH, Villamizar Durán y otros vs. Colombia, Sentencia de 20 de noviembre de 2018 (Excepción Preliminar, Fondo, Reparaciones y Costas), serie C, No. 364, párrs. 64 y 65 (donde se describe la doctrina de la "seguridad nacional" utilizada en Colombia en contra de los defensores de derechos humanos, entre ellos sindicalistas y miembros de movimientos de reivindicación campesina); Corte IDH, Caso Isaza Uribe y otros vs. Colombia, Sentencia de 20 de noviembre de 2018 (Fondo, Reparaciones y Costas), serie C, No. 363, párrs. 127, 128, 144 y 207; Corte IDH, Caso Goiburú y otros vs. Paraguay, Sentencia de 22 de septiembre de 2006 (Fondo, Reparaciones y Costas), serie C, No. 153, párr. 61.5 (donde se describe el uso por los gobiernos dictatoriales del Cono Sur de la "doctrina de seguridad nacional" contra movimientos de izquierda y otros grupos considerados como "enemigos comunes"); Corte IDH, Caso Escher y otros vs. Brasil, serie C, No. 200, *supra,* nota 44 (opinión concurrente del juez Sergio García Ramírez, párr. 13, donde señala: "Para favorecer sus excesos, las tiranías 'clásicas' —permítaseme calificarlas así— que abrumaron a muchos países de nuestro hemisferio, invocaron motivos de seguridad nacional, soberanía, paz pública [...]. En aquellas invocaciones había un manifiesto componente ideológico; atrás operaban intereses poderosos. Otras formas de autoritarismo, más de esta hora, invocan la seguridad pública, la lucha contra la delincuencia, para imponer restricciones a los derechos y justificar el menoscabo de la libertad"); Corte IDH, Caso Chitay Nech y otros vs. Guatemala, serie C, No. 212, *supra,* nota 107, párr. 64 (donde se describe la "Doctrina de Seguridad Nacional" aplicada en Guatemala "a toda persona u organización que representara cualquier forma de oposición al Estado"); Corte IDH, Caso de la Masacre de Las Dos Erres vs. Guatemala, Sentencia de 24 de noviembre de 2009 (Excepción Preliminar, Fondo, Reparaciones y Costas), serie C, No. 211, párrs. 71 a 73 (donde se describe la misma doctrina).

141 Véase, por ejemplo, CIDH, Informe No. 57/19, *supra,* nota 3, párr. 64 (donde se menciona un discurso de Uribe en el cual el presidente afirmó que la labor de la CCAJAR era una "excusa para dar cobertura a los terroristas); *Personas defensoras de derechos humanos en Colombia*, *supra,* nota 6, párrs. 137 a 140 (donde se catalogan campañas llevadas a cabo por funcionarios públicos durante varios años para desprestigiar a defensores de derechos humanos).

especificar claramente los criterios que deben aplicarse para determinar los casos en los cuales este tipo de limitaciones resulta legítimo”[142].

Por último, en la Convención Americana se establecen los principios de necesidad y proporcionalidad, de acuerdo con los cuales las medidas de vigilancia estatal deben ser necesarias, idóneas y proporcionales en el contexto particular, de manera tal que sean “necesarias en una sociedad democrática”[143]. De hecho, hay consenso internacional en que la injerencia en los derechos resultante de la vigilancia estatal debe ser necesaria y proporcional[144]. Aunque esta Corte no ha tenido la ocasión de explayarse sobre estos principios en el contexto de la vigilancia[145], ha considerado que las medidas son “necesarias” en los casos en “que sean absolutamente indispensables para conseguir el fin deseado y que no exista una medida menos gravosa respecto al derecho intervenido entre todas aquellas que cuentan con la misma idoneidad para alcanzar el objetivo propuesto”[146]. Además, esta Corte ha señalado que la injerencia en los derechos es proporcional cuando “el sacrificio inherente a la restricción [...] no resulte exagerado o desmedido frente a las ventajas que se obtienen mediante tal restricción y el cumplimiento de la finalidad perseguida”[147].

b. Esta Corte debería reafirmar que la vigilancia masiva es incompatible con las normas internacionales de derechos humanos

Varios expertos y órganos internacionales en el ámbito de los derechos humanos están de acuerdo en que la vigilancia masiva, a diferencia de la vigilancia específica, es intrínsecamente violatoria de los principios de necesidad y proporcionalidad y, por consiguiente, socava la esencia del derecho a la privacidad. Esta Corte debería sumarse a esa afirmación. La Comisión Interamericana ha señalado que la vigilancia masiva de las comunicaciones “en ningún caso

---

[142] *Declaración conjunta sobre la vigilancia*, *supra,* nota 77, párr. 9.

[143] Convención Americana sobre Derechos Humanos, *supra,* nota 50, arts. 11.2, 13.2 y 16.2. Véase también Corte IDH, Caso Escher y otros vs. Brasil, serie C, No. 200, *supra,* nota 44, párr. 116; Corte IDH, Caso Tristán Donoso vs. Panamá, serie C, No. 193, *supra,* nota 122, párr. 56.

[144] Véase TEDH, Szabo, App. No. 37138/14, *supra,* nota 128, párrs. 54 y 55; TJUE, Asunto C-293/12, Digital Rights Ireland, Ltd. v. Minister for Communications, ECLI:EU:C:2014:238, párr. 46 (8 de abril de 2014) [en adelante “TJUE, Asunto C-293/12, DRI v. Minister”]; Comité de Derechos Humanos, *Van Hulst v. Netherlands*, U.N. Doc. CCPR/C/82/D/903/1999, párr. 7.6 (1 de noviembre de 2004); *Observaciones finales del Comité de Derechos Humanos sobre Estados Unidos*, *supra,* nota 39, párr. 22.d; Informe de 2018 del Alto Comisionado para los Derechos Humanos, *supra,* nota 51, párr. 10; Consejo de Derechos Humanos, *Informe de Martin Scheinin, Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo*, párrs. 17 y 18, U.N. Doc. A/HRC/13/37 (28 de diciembre de 2009); *Principios de Johannesburgo sobre seguridad nacional, libertad de expresión y acceso a información*, principio 1.3, U.N. Doc. E/CN.4/1996/39 (22 de marzo de 1996). Véase también Tribunal Africano de Derechos Humanos y de los Pueblos, Umuhoza v. Rwanda, párr. 132 (24 de noviembre de 2017).

[145] Corte IDH, Caso Escher y otros vs. Brasil, serie C, No. 200, *supra,* nota 44, párr. 146.

[146] Corte IDH, Caso Chaparro Álvarez y Lapo Íñiguez vs. Ecuador, Sentencia de 21 de noviembre de 2007 (Excepciones Preliminares, Fondo, Reparaciones y Costas), serie C, No. 189, párr. 93. El Tribunal Europeo de Derechos Humanos ha adoptado una norma similar en materia de necesidad. Véase, por ejemplo, TEDH, Faber v. Germany, App. No. 40721/08, párr. 32, 43 (24 de julio de 2012), https://hudoc.echr.coe.int/eng?i=001-112446 (donde se señala que la prueba de la necesidad en una sociedad democrática requiere que el Tribunal determine si la injerencia en los derechos a la libertad de expresión y a la libertad de reunión pacífica corresponde a una necesidad social urgente y que el Estado tiene que cumplir la obligación positiva de proteger el derecho de reunión, para lo cual debe buscar el medio menos restrictivo posible).

[147] Corte IDH, Caso Chaparro Álvarez y Lapo Íñiguez vs. Ecuador, serie C, No. 189, *supra,* nota 146, párr. 93 (donde se examina la proporcionalidad de la restricción del derecho a la libertad). Véase también Corte IDH, Caso Kimel vs. Argentina, serie C, No. 177, *supra,* nota 64, párrs. 83 y 94 (donde se aplica esta prueba al examen de la proporcionalidad de la restricción del derecho a la libertad de pensamiento y de expresión); Corte IDH, Caso Claude Reyes vs. Chile, serie C, No. 151, *supra,* nota 87, párr. 91.

podrá ser considerada como proporcional"[148]. Los órganos de las Naciones Unidas en la materia también han reconocido la incompatibilidad inherente entre la vigilancia masiva y las normas sobre derechos humanos[149]. En el contexto de la retención, el acceso y la transferencia de datos de las comunicaciones, el Tribunal de Justicia de la Unión Europea ha reconocido en repetidas ocasiones que el *acceso* indiscriminado (o no específico) a metadatos retenidos por proveedores de servicios de comunicaciones o su *transmisión* a órganos de inteligencia, incluso para combatir "delitos graves" o "proteger la seguridad nacional", no es permisible[150]. El Tribunal ha dictaminado asimismo que la *retención* indiscriminada de datos de tráfico y de localización para cualquier fin que no sea proteger la seguridad nacional no es permisible[151]. A lo largo de su historia, el Tribunal Europeo de Derechos Humanos también ha expresado preocupación con respecto a la vigilancia masiva en el ámbito nacional[152]. Más recientemente, en el contexto del régimen del Reino Unido de interceptación masiva en la esfera *internacional*, el Tribunal concluyó que tal régimen era violatorio de los derechos a la privacidad y a la libertad de expresión, pero se abstuvo de dictaminar que fuese desproporcionado en sí mismo[153], lo cual se opone al consenso internacional[154] y a las críticas formuladas por el Comité de Derechos Humanos en relación con el régimen de vigilancia del Reino Unido, que permite la interceptación en masa de comunicaciones y aplica protecciones menos estrictas a las comunicaciones internacionales que a las nacionales[155].

c. La vigilancia de las comunicaciones debe efectuarse con autorización judicial previa y supervisión independiente para evitar abusos

---

[148] CIDH, *La CIDH y su Relatoría Especial para la Libertad de Expresión exhortan al Estado de Colombia a establecer una investigación diligente, oportuna e independiente respecto a las denuncias sobre espionaje ilegal a periodistas, operadores de justicia, personas defensoras de derechos humanos y líderes políticos*, Comunicado de Prensa 118/20 (21 de mayo de 2020), https://www.oas.org/es/cidh/prensa/Comunicados/2020/118.asp.

[149] Comité de Derechos Humanos, *Observaciones finales sobre el sexto informe periódico de Hungría*, párr. 43, U.N. Doc. CCPR/C/HUN/CO/6 (9 de mayo de 2018) [en adelante *Observaciones finales del Comité de Derechos Humanos sobre Hungría*] (donde dice: "Preocupa al Comité que el marco jurídico del Estado parte sobre la vigilancia secreta por motivos de seguridad nacional [...] permita la interceptación masiva de comunicaciones"); Informe de 2018 del Alto Comisionado para los Derechos Humanos, *supra,* nota 51, párr. 17 (donde se señala que la vigilancia en masa e indiscriminada "no es permisible en virtud del derecho internacional de los derechos humanos, ya que no sería posible realizar un análisis individualizado de la necesidad y la proporcionalidad en el contexto de esas medidas"); Organización para la Seguridad y Cooperación en Europa, *Joint Declaration on Freedom of Expression and Responses to Conflict Situations*, párr. 8.a (4 de mayo de 2015), http://www.osce.org/fom/154846 [en adelante *Joint Declaration on Freedom of Expression*].

[150] TJUE, Asunto C-623/17, Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others, ECLI:EU:C:2020:790, párrs. 78 a 81 (6 de octubre de 2020) [en adelante "TJUE, Asunto C-623/17, Privacy International v. Secretary of State"]; TJUE, Asunto C-140/20, G.D. v. Commissioner of An Garda Síochána and others, ECLI:EU:C:2022:258, párr. 105 (5 de abril de 2021).

[151] TJUE, Asunto C-293/12, DRI v. Minister*, supra,* nota 144, párrs. 56 a 59. El Tribunal de Justicia de la Unión Europea ha rechazado la retención indiscriminada de metadatos para combatir delitos graves, pero ha permitido que los Estados requieran que los proveedores de servicios de comunicaciones conserven de manera indiscriminada datos de tráfico y de localización para "proteger la seguridad nacional" en el marco de estrictas salvaguardias, entre ellas una revisión efectiva por un órgano independiente. Véase TJUE, Asuntos acumulados C-511/18, C-512/18 y C-520/18, La Quadrature du Net v. Premier Ministre, ECLI:EU:C:2020:791, párrs. 137 a 139 (6 de octubre de 2020) [en adelante "TJUE, Asuntos acumulados C-511/18 y C-520/18, La Quadrature du Net"].

[152] Véase, por ejemplo, TEDH*,* Szabo, App. No. 37138/14, *supra,* nota 128, párr. 67 (donde se expresa grave preocupación por la posibilidad de la vigilancia ilimitada de un gran número de ciudadanos).

[153] TEDH, Big Brother Watch, App. No. 58170/13, *supra,* nota 123, párr. 376.

[154] *Id.*, párr. 11 (opinión en parte concordante y en parte discordante del juez Pinto de Albuquerque, en la cual se observa que, si hay un consenso en Europa sobre la interceptación masiva, no dirigida a un usuario en particular, el consenso es que debe prohibirse, pero el Tribunal Europeo de Derechos Humanos no ha prestado atención a este asunto).

[155] Comité de Derechos Humanos, *Observaciones finales sobre el séptimo informe periódico del Reino Unido de Gran Bretaña e Irlanda del Norte*, párr. 24, U.N. Doc. CCPR/C/GBR/CO/7 (17 de agosto de 2015) [en adelante *Observaciones finales del Comité de Derechos Humanos sobre el Reino Unido*].

Esta Corte ha reafirmado la importancia de la aplicación de medidas de control "rigurosas" a los servicios de inteligencia y sus actividades[156]. Aunque, de acuerdo con la Constitución de Colombia, se requiere una orden judicial para interceptar o registrar comunicaciones privadas[157], la ley estatutaria colombiana —la Ley de Inteligencia— exime a los órganos de inteligencia de este requisito en los casos en que el acto forme parte de otras actividades de vigilancia, como monitoreo del espectro electromagnético y acceso a datos retenidos por proveedores de servicios de comunicaciones[158]. Si bien esta Corte no ha tenido la oportunidad de explayarse sobre las normas precisas requeridas para la autorización apropiada o la supervisión de la vigilancia de comunicaciones de conformidad con la Convención Americana, la jurisprudencia interamericana de larga data sobre protecciones del debido proceso y los antecedentes preocupantes de vigilancia abusiva en Colombia deberían llevar a esta Corte a disponer que se exija autorización *judicial previa* para *toda* actividad de vigilancia en Colombia[159]. Además, esta Corte debería sumarse al consenso internacional de que los regímenes de vigilancia deben operar bajo la supervisión efectiva de un órgano externo independiente[160].

El Tribunal Europeo de Derechos Humanos, el Comité de Derechos Humanos y diversos expertos en la materia están de acuerdo en que la supervisión de las actividades de vigilancia debe estar a cargo de órganos independientes y abarcar varias etapas. En el examen de un régimen de vigilancia para prevenir o detectar delitos, salvaguardar intereses económicos y proteger la seguridad nacional, el Tribunal indicó tres etapas en las cuales la supervisión independiente es crucial: cuando se ordena la vigilancia, cuando se la está llevando a cabo y una vez concluida[161]. Asimismo, el Comité ha recalcado la importancia de un proceso para autorizar la vigilancia de las comunicaciones y ha encomendado a los Estados que establezcan mecanismos independientes de supervisión efectiva de los regímenes de vigilancia[162]. Estas salvaguardias procesales se basan en el consenso internacional.

Hay tres razones principales por las cuales esta Corte debería respaldar el requisito de la autorización judicial previa de la vigilancia estatal de las comunicaciones. Primero, hay consenso internacional en que la autorización judicial previa de toda actividad de vigilancia es una

---

156 Corte IDH, Caso Myrna Mack Chang vs. Guatemala, Sentencia de 25 de noviembre de 2003 (Fondo, Reparaciones y Costas), serie C, No. 101, párr. 284.

157 CONSTITUCIÓN POLÍTICA DE LA REPÚBLICA DE COLOMBIA, art. 15, http://www.secretariasenado.gov.co/constitucion-politica.

158 Véase el apartado B.2.a.

159 Esta Corte ha requerido orden judicial previa para proteger los derechos de personas arrestadas y detenidas (Corte IDH, Caso Maritza Urrutia vs. Guatemala, Sentencia de 27 de noviembre de 2003 [Fondo, Reparaciones y Costas], serie C, No. 103, párr. 67) sometidas a cacheo (Corte IDH, Caso Fernández Prieto y Tumbeiro vs. Argentina, Sentencia de 1 de septiembre de 2020 [Fondo, Reparaciones y Costas], serie C, No. 411, párr. 109) y para garantizar el derecho a la privacidad (Corte IDH, Caso Escué Zapata vs. Colombia, Sentencia de 4 de julio de 2007 [Fondo, Reparaciones y Costas], serie C, No. 165, párr. 94).

160 TEDH, Big Brother Watch, App. No. 58170/13, *supra,* nota 123, párr. 197. Véase también *Observaciones finales del Comité de Derechos Humanos sobre Belarús*, *supra,* nota 123, párr. 44; resolución 68/167 de la Asamblea General, párr. 4 (18 de diciembre de 2013); *Declaración conjunta sobre la vigilancia*, *supra,* nota 77, párr. 9; Informe de 2019 del Relator Especial sobre el derecho a la privacidad, *supra,* nota 36, párr. 46.b.

161 TEDH, Big Brother Watch, App. No. 58170/13, *supra,* nota 123, párr. 336.

162 *Observaciones finales del Comité de Derechos Humanos sobre Belarús*, *supra,* nota 123, párr. 44; *Observaciones finales del Comité de Derechos Humanos sobre Hungría*, *supra,* nota 149, párr. 44. Véase también *Declaración conjunta sobre la vigilancia*, *supra,* nota 77, párr. 9.

importante salvaguardia contra la arbitrariedad[163]. Al respecto, la Comisión Interamericana ha adoptado lo establecido por el Relator Especial de la CIDH para la Libertad de Expresión al respecto:

> ... las decisiones de realizar tareas de vigilancia que invadan la privacidad de las personas *deben ser autorizadas por autoridades judiciales independientes*, que deben dar cuenta de las razones por las cuales la medida es idónea para alcanzar los fines que persigue en el caso concreto; de si es lo suficientemente restringida para no afectar el derecho involucrado más de lo necesario; y de si resulta proporcional respecto del interés que se quiere promover. [...] Los Estados deben garantizar que la autoridad judicial sea especializada y competente para tomar decisiones judiciales sobre la legalidad de la vigilancia de las comunicaciones, las tecnologías utilizadas y su impacto en el ámbito de los derechos que pueden resultar comprometidos[164].

Segundo, la exigencia de orden judicial previa se fundamenta también en la jurisprudencia interamericana de larga data relativa a las protecciones del debido proceso[165]. Esta Corte ha entendido que las garantías judiciales establecidas en el artículo 8 de la Convención Americana constituyen "'[e]l conjunto de requisitos que deben observarse en las instancias procesales' a efecto de que las personas puedan defenderse adecuadamente ante cualquier acto emanado del Estado que pueda afectar sus derechos"[166]. Esta Corte debería considerar la autorización judicial previa como una protección necesaria contra el "riesgo intrínseco de abuso" de un sistema de vigilancia secreta[167].

---

163 TEDH, Big Brother Watch, App. No. 58170/13, *supra,* nota 123, párr. 351. Véase también TEDH, Roman Zakharov, App. No. 47143/06, *supra,* nota 39, párr. 249; TEDH, Szabo, App. No. 37138/14, *supra,* nota 128, párr. 77; Comité de Derechos Humanos, *Observaciones finales sobre el séptimo informe periódico de Alemania*, párr. 43, U.N. Doc. CCPR/C/DEU/CO/7 (11 de noviembre de 2021). Ni el Tribunal Europeo de Derechos Humanos ni el Tribunal de Justicia de la Unión Europea han requerido autorización *judicial* previa de las medidas de vigilancia, a pesar de que reconocen que es una importante salvaguardia, pero han requerido autorización *independiente* previa. Véase TEDH, Big Brother Watch, App. No. 58170/13, *supra,* nota 123, párr. 351 (donde dice que la interceptación a gran escala debe ser autorizada por un órgano que sea independiente del Poder Ejecutivo); TJUE, Asunto C-293/12, DRI v. Minister, *supra,* nota 144, párr. 62 (donde se señala que, para proteger el respeto de la vida privada, el acceso de las autoridades estatales a datos conservados por proveedores de servicios de comunicaciones debe estar supeditado "a un control previo efectuado, bien por un órgano jurisdiccional, bien por un organismo administrativo autónomo, cuya decisión tenga por objeto limitar el acceso a los datos y su utilización a lo estrictamente necesario para alcanzar el objetivo perseguido"). Véase también TJUE, Asuntos acumulados C-203/15 y C-698/15, Tele2 v. Post-och, *supra,* nota 82, párr. 120 (donde se señala que "es esencial que el acceso de las autoridades nacionales competentes a los datos conservados esté sujeto, en principio, salvo en casos de urgencia debidamente justificados, a un control previo de un órgano jurisdiccional o de una entidad administrativa independiente"); TJUE, Asunto C-623/17, Privacy International v. Secretary of State, *supra,* nota 150, párrs. 78 a 82 (donde se confirma que se aplica la jurisprudencia de la Unión Europea, incluidos los asuntos acumulados C-203/15 y C-698/15, Tele2 v. Post-och, cuando los órganos de inteligencia procuran obtener datos retenidos por proveedores de servicios de telecomunicaciones con fines relacionados con la seguridad nacional).

164 Informe de 2013 del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión*, supra,* nota 78, párr. 165 (énfasis añadido). Véase Informe No. 57/19, *supra,* nota 3, párrs. 308 y 312 (donde se respalda la posición del Relator Especial). Véase también CIDH, *Derecho a la información y seguridad nacional*, párr. 58, OEA/Ser.L/V/II CIDH/RELE/INF.24/20 (julio de 2020) [en adelante "Informe de 2020 del Relator Especial de la CIDH para la Libertad de Expresión"] (se debe exigir autorización judicial previa para las actividades de vigilancia).

165 Informe de 2013 de la Relatora Especial de la CIDH para la Libertad de Expresión*, supra,* nota 78, párrs. 164 y 165 (donde se recurre al artículo 8 de la Convención Americana sobre Derechos Humanos para establecer el requisito de la autorización judicial previa).

166 Corte IDH, Caso Ivcher Bronstein vs. Perú, Sentencia de 6 de febrero de 2001 (Reparaciones y Costas), serie C, No. 74, párr. 102 (citas omitidas).

167 Corte IDH, Caso Escher y otros vs. Brasil, serie C, No. 200, *supra,* nota 44, párr. 118.

Asimismo, esta Corte ha recalcado que el derecho a la privacidad requiere una sólida protección[168]. En el caso Escher contra Brasil, esta Corte puso de relieve la importancia de la supervisión independiente de la vigilancia de las comunicaciones y el destacado papel de los jueces en el examen *ex parte* de solicitudes de medidas de vigilancia:

> En los procedimientos cuya naturaleza jurídica exija que la decisión sea emitida sin audiencia de la otra parte, la motivación y fundamentación deben demostrar que han sido ponderados todos los requisitos legales y demás elementos que justifican la concesión o la negativa de la medida. De ese modo, el libre convencimiento del juez debe ser ejercido respetándose las garantías adecuadas y efectivas contra posibles ilegalidades y arbitrariedades en el procedimiento en cuestión[169].

En tercer lugar, el largo historial de Colombia de espionaje de opositores políticos también justifica el requisito de un control judicial para prevenir el abuso[170]. En el caso Myrna Mack Chang contra Guatemala, esta Corte reconoció el peligro inherente de la vigilancia secreta y afirmó que "[l]as medidas tendientes a controlar las labores de inteligencia deben ser especialmente rigurosas, puesto que, dadas las condiciones de reserva bajo las que se realizan esas actividades, pueden derivar hacia la comisión de violaciones de los derechos humanos y de ilícitos penales"[171]. Asimismo, el Tribunal Europeo de Derechos Humanos ha reconocido que el control judicial ofrece las mejores garantías de independencia e imparcialidad y un procedimiento apropiado, en particular en un campo en el cual podría ser muy fácil cometer abusos, lo cual podría tener consecuencias perniciosas para la sociedad democrática en conjunto[172]. El expediente que obra en poder de esta Corte demuestra que Colombia ha llevado a cabo una vigilancia abusiva durante décadas. Por lo tanto, esta Corte debería requerir que el país adopte las mejores garantías de independencia que tenga a su alcance.

Aunque la autorización judicial previa es necesaria, es solo una parte de un mecanismo de supervisión efectiva, ya que se pueden cometer abusos después que se otorga la autorización[173]. A nivel internacional, hay consenso en el sentido de que los regímenes de vigilancia también deben estar supervisados regularmente, después de la autorización, por órganos externos interdependientes[174]. Según las mejores prácticas internacionales:

---

168 Corte IDH, Caso Escué Zapata vs. Colombia, serie C, No. 165, *supra,* nota 159, párr. 95 (donde dice: "La protección de la vida privada, la vida familiar y el domicilio de injerencias arbitrarias o abusivas implica el reconocimiento de que existe un ámbito personal que debe estar exento e inmune a las invasiones o agresiones abusivas o arbitrarias por parte de terceros o de la autoridad pública").

169 Corte IDH, Caso Escher y otros vs. Brasil, serie C, No. 200, *supra,* nota 44, párr. 139.

170 Véase, por ejemplo, TEDH, Ekimdzhiev, App. No. 70078/12, *supra,* nota 120, párr. 293 (donde se argumenta que los tribunales deberían tener en cuenta la existencia o la ausencia de un abuso real al examinar el sistema de vigilancia de un Estado a la luz de las normas internacionales de derechos humanos).

171 Corte IDH, Caso Myrna Mack Chang vs. Guatemala, serie C, No. 101, *supra,* nota 156, párr. 284.

172 TEDH, Szabo, App. No. 37138/14, *supra,* nota 128, párr. 77.

173 Informe de 2014 del Alto Comisionado para los Derechos Humanos, *supra,* nota 45, párr. 38 (donde se señala que "la intervención judicial en la supervisión tampoco debe considerarse una panacea; en varios países, el mandamiento o la revisión judicial de las actividades de vigilancia digital de los servicios de inteligencia y/o los organismos encargados de hacer cumplir la ley han supuesto en la práctica un mero ejercicio de aprobación sumisa. Por consiguiente, la atención se está centrando cada vez más en modelos mixtos de supervisión administrativa, judicial y parlamentaria").

174 TEDH, Ekimdzhiev, App. No. 70078/12, *supra,* nota 120, párrs. 334 a 347 (donde se examinan la independencia y la efectividad de los mecanismos de supervisión por separado del examen de los procedimientos de autorización); *Observaciones finales del Comité de Derechos Humanos sobre Belarús*, *supra,* nota 123, párr. 44; *Observaciones finales del Comité de Derechos Humanos sobre Hungría*, *supra,* nota 149, párr. 44. Véase también resolución 68/167 de la Asamblea General, párr. 4.d (18 de diciembre de 2013); *Declaración conjunta sobre la vigilancia*, *supra,* nota 77, párr. 9.

> Los marcos de supervisión pueden estar compuestos por una combinación de medidas de supervisión administrativa, judicial y/o parlamentaria. Los órganos de supervisión deben ser independientes de las autoridades que llevan a cabo la vigilancia y disponer de conocimientos técnicos, competencias y recursos pertinentes y adecuados. La autorización y la supervisión deben estar a cargo de distintas instituciones. Los organismos de supervisión independientes deben investigar y supervisar de forma proactiva las actividades de las entidades que realizan la vigilancia, tener acceso a los resultados de la vigilancia y llevar a cabo exámenes periódicos de las capacidades de vigilancia y los avances tecnológicos. Los organismos que llevan a cabo la vigilancia deben tener la obligación de facilitar toda la información necesaria para una supervisión eficaz cuando se les solicite y de presentar informes periódicos a los órganos de supervisión, así como de llevar registros de todas las medidas de vigilancia adoptadas. Los procesos de supervisión también deben ser transparentes y estar sujetos a escrutinio público adecuado, y las decisiones de los órganos de supervisión deben poder ser objeto de recurso o de revisión independiente[175].

Las víctimas de vigilancia ilegal de las comunicaciones deben contar con recursos efectivos, para lo cual es necesario que se notifique la vigilancia y que se pueda corregir o borrar la información recopilada El artículo 25 de la Convención Americana dispone que "[t]oda persona tiene derecho a un recurso sencillo y rápido o a cualquier otro recurso efectivo ante los jueces o tribunales competentes, que la ampare contra actos que violen sus derechos fundamentales reconocidos por la Constitución, la ley o la presente Convención"[176]. Esta Corte ha descrito este derecho como "uno de los pilares básicos, no sólo de la Convención Americana, sino del propio Estado de Derecho en una sociedad democrática"[177] y ha señalado que "[e]l acceso a la justicia constituye una norma imperativa de Derecho Internacional"[178]. De acuerdo con el principio de protección judicial efectiva y con la arraigada jurisprudencia de esta Corte, la Convención Americana obliga a los Estados a establecer recursos judiciales que "sean accesibles para las partes, sin obstáculos o demoras indebidas, a fin de que alcancen su objetivo de manera rápida, sencilla e integral"[179]. Los recursos deben ser efectivos, es decir, deben ofrecer una posibilidad real de reparar violaciones de derechos humanos[180]. Esta Corte ha concluido que "[l]a inexistencia de un recurso efectivo frente a las violaciones de los derechos recogidos en la Convención supone una transgresión de la misma por el Estado Parte"[181]. Esta Corte debe

---

[175] Informe de 2018 del Alto Comisionado para los Derechos Humanos, *supra,* nota 51, párr. 40. Véase también *Principios globales sobre seguridad nacional y el derecho a la información ("Principios de Tshwane")*, OPEN SOCIETY JUSTICE INITIATIVE, Principio 31 (2013), https://www.oas.org/es/sla/ddi/docs/acceso_informacion_Taller_Alto_Nivel_Paraguay_2018_documentos_referencia_Principios_Tshwane.pdf [en adelante "Principios de Tshwane"]; Informe de 2010 del Relator Especial sobre la protección y la promoción de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, *supra,* nota 2, párr. 13, Práctica 7; resolución 75/291 de la Asamblea General, *Estrategia Global de las Naciones Unidas contra el Terrorismo: séptimo examen*, párr. 106, U.N. Doc. A/RES/75/291 (30 de julio de 2021).

[176] Convención Americana sobre Derechos Humanos, *supra,* nota 50, art. 25. Véase también resolución 217A (III) de la Asamblea General, Declaración Universal de Derechos Humanos, art. 8, (1948); Convención Internacional sobre la Protección de los Derechos de Todos los Trabajadores Migratorios y de sus Familiares art. 2.3, 18 de diciembre de 1990, 2220 U.N.T.S. 3; Declaración Americana de los Derechos y Deberes del Hombre, art. XVIII, OEA/Ser.LV/I.4 Rev. (1965).

[177] Corte IDH, Caso Castillo Páez vs. Perú, Sentencia de 3 de noviembre de 1997 (Fondo), serie C, No. 34, párr. 82.

[178] Corte IDH, Caso Goiburú y otros vs. Paraguay, serie C, No. 153, *supra,* nota 140, párr. 131.

[179] Corte IDH, Caso Lagos del Campo vs. Perú, Sentencia de 31 de agosto de 2013 (Excepciones Preliminares, Fondo, Reparaciones y Costas), serie C, No. 340, párr. 174.

[180] Corte IDH, Caso Velásquez Rodríguez vs. Honduras, Sentencia de 26 de junio de 1987 (Excepciones Preliminares), serie C, No. 1, párr. 93; Caso Comunidad Indígena Xákmok Kásek vs. Paraguay, Sentencia de 24 de agosto de 2010 (Fondo, Reparaciones y Costas), serie C, No. 214, párr. 140; Caso Abrill Alosilla y otros vs. Perú, Sentencia de 4 de marzo de 2011 (Fondo, Reparaciones y Costas), serie C, No. 223, párr. 75.

[181] Corte IDH, Caso Pueblos Kaliña y Lokono Peoples vs. Surinam, Sentencia de 25 de noviembre de 2015 (Fondo, Reparaciones y Costas), serie C, No. 309, párr. 237.

determinar si las leyes colombianas ofrecen a las víctimas de vigilancia estatal ilegal recursos efectivos acordes con esta jurisprudencia afianzada[182].

La notificación es una *conditio sine qua non* para asegurar el derecho de las personas a impugnar la vigilancia de las comunicaciones. Tanto en asuntos penales como en el ámbito de la inmigración, esta Corte ha sostenido que la falta de notificación infringe las garantías judiciales establecidas por el artículo 8 de la Convención Americana[183]. De acuerdo con esta jurisprudencia interamericana, la Corte debería establecer la obligación de notificar acerca de la vigilancia. Esta Corte ha afirmado en reiteradas ocasiones que las garantías mínimas establecidas en el artículo 8 de la Convención Americana constituyen el debido proceso "para la determinación de sus derechos y obligaciones de orden civil, laboral, fiscal o de cualquier otro carácter"[184]. Asimismo, esta Corte ha entendido que los requisitos del debido proceso "deben observarse en las instancias procesales a efectos de que las personas estén en condiciones de defender adecuadamente sus derechos ante cualquier acto del Estado, adoptado por cualquier autoridad pública, sea administrativa, legislativa o judicial, que pueda afectarlos"[185].

En el caso Szabo contra Hungría, al examinar el marco jurídico de la recopilación de inteligencia dentro del país con fines de seguridad nacional, el Tribunal Europeo de Derechos Humanos destacó el importante papel de la notificación cuando afirmó que, en principio, había poco margen para que la persona del caso interpusiera un recurso de cualquier tipo si no se le avisaba sobre las medidas tomadas sin su conocimiento y, por consiguiente, la persona no podía impugnar su justificación en retrospectiva[186]. Asimismo, el Tribunal de Justicia de la Unión Europea, en un caso de impugnación de la retención indiscriminada de metadatos por proveedores de servicios de comunicaciones y acceso irrestricto de las autoridades estatales a esos metadatos, afirmó que la notificación de las personas cuyos datos habían sido accesados por

---

[182] El Tribunal Europeo de Derechos Humanos ha incluido el acceso a recursos efectivos entre los componentes de su evaluación de todo régimen de vigilancia secreta. Véase TEDH, Ekimdzhiev, App. No. 70078/12, *supra,* nota 120, párrs. 352 a 355 (donde se determina si el régimen de vigilancia búlgaro ofrecía un recurso efectivo a las personas que se quejaban de ser objeto de vigilancia ilegal).

[183] Véase, por ejemplo, Corte IDH, Caso Vélez Loor vs. Panamá, Sentencia de 23 de noviembre de 2010 (Excepciones Preliminares, Fondo, Reparaciones y Costas), serie C, No. 218, párr. 180 (donde se afirma que la falta de notificación a un detenido de su derecho a apelar creó un estado de incertidumbre jurídica que "tornó impracticable el ejercicio del derecho a recurrir del fallo sancionatorio" y constituyó en sí misma una violación de la Convención); Corte IDH, Caso Tibi vs. Ecuador, Sentencia de 7 de septiembre de 2004 (Excepciones Preliminares, Fondo, Reparaciones y Costas), serie C, No. 114, párrs. 185, 188 y 189 (donde se señala que la víctima "no tuvo conocimiento oportuno y completo" de los cargos penales que se le imputaban, lo cual lo privó de la oportunidad de preparar su defensa de manera adecuada y constituyó una violación de la Convención Americana); Corte IDH, Caso López Álvarez vs. Honduras, Sentencia de 1 de febrero de 2006 (Fondo, Reparaciones y Costas), serie C, No. 141, párr. 149; Corte IDH, Caso Barreto Leiva vs. Venezuela, Sentencia de 17 de noviembre de 2009 (Fondo, Reparaciones y Costas), serie C, No. 206, párr. 28.

[184] Corte IDH, Caso del Tribunal Constitucional vs. Perú, Sentencia de 31 de enero de 2001 (Fondo, Reparaciones y Costas), serie C, No. 71, párr. 70. Véase también Corte IDH, Caso Ivcher Bronstein vs. Perú, serie C, No. 74, *supra,* nota 166, párr. 103; Corte IDH, Caso Vélez Loor vs. Panamá, serie C, No. 218, *supra,* nota 183, párr. 142; Corte IDH, Caso Nadege Dorzema y otros vs. República Dominicana, Sentencia de 24 de octubre de 2012 (Fondo, Reparaciones y Costas), serie C, No. 251, párr. 157; Corte IDH, Caso del Tribunal Constitucional (Camba Campos y otros) vs. Ecuador, Sentencia de 28 de agosto de 2013 (Excepciones Preliminares, Fondo, Reparaciones y Costas), serie C, No. 268, párr. 166; Corte IDH, Caso Familia Pacheco Tineo vs. Estado Plurinacional de Bolivia, Sentencia de 25 de noviembre de 2013 (Excepciones Preliminares, Fondo, Reparaciones y Costas), serie C, No. 272, párr. 130.

[185] Corte IDH, Caso Ruano Torres y otros vs. El Salvador, Sentencia de 5 de octubre de 2015 (Fondo, Reparaciones y Costas), serie C, No. 303, párr. 151.

[186] TEDH*,* Szabo, App. No. 37138/14, *supra,* nota 128, párr. 86. Como en las leyes húngaras no se disponía la notificación de ningún tipo ni recursos en casos de abuso, el Tribunal Europeo de Derechos Humanos concluyó que las leyes no ofrecían salvaguardias adecuadas. *Id*.

las autoridades estatales era “necesaria para que dichas personas puedan ejercer, concretamente, su derecho a la tutela judicial efectiva” de conformidad con la directiva europea sobre privacidad[187]. Concluyó que “es necesario que las autoridades nacionales competentes a las que se conceda el acceso a los datos conservados informen de ello a las personas afectadas, [...] siempre que esa comunicación no pueda comprometer las investigaciones que llevan a cabo esas autoridades”[188].

El Tribunal Europeo de Derechos Humanos ha aceptado en algunos casos que, en vez de notificar, los Estados simplemente aseguren que cualquiera que “sospeche” que lo han vigilado tenga legitimación procesal[189]. Si bien es una importante salvaguardía contra el abuse asegurar que en el derecho colombiano se prevea la legitimación para impugnar la vigilancia ilegal de aquellos que sospechen que los han vigilado —aunque no lo sepan con certeza—, no es suficiente. Las actividades de vigilancia por órganos de inteligencia dirigidas a defensores de derechos humanos no se descubrieron hasta años después[190]. Aunque algunos tenían razones para sospechar que los estaban vigilando, otros, como los familiares de miembros de la CCAJAR, no las tenían. Por lo tanto, esta Corte debería examinar el enfoque más protector aplicado por el Tribunal Europeo de Derechos Humanos en el caso Szabo contra Hungría[191] y refrendado por el Tribunal de Justicia de la Unión Europea.

El derecho a un recurso efectivo frente a la vigilancia estatal ilegal requiere también que las personas vigiladas tengan acceso a los datos recopilados por el gobierno y puedan corregirlos o borrarlos. La Comisión Interamericana incorporó este requisito en su Declaración de Principios sobre Libertad de Expresión[192]. Los tribunales europeos y los expertos en derechos humanos han reafirmado esta obligación en casos de interceptación de comunicaciones y transferencia de datos personales[193] y han recalcado este requisito en el contexto de la vigilancia de comunicaciones entre abogados y clientes[194].

d. *El público debe tener acceso a la información sobre prácticas de vigilancia estatal, lo cual constituye una salvaguardia crucial contra el abuso*

---

187 TJUE, Asuntos acumulados C-203/15 y C-698/15, Tele2 v. Post-och, *supra,* nota 82, párr. 121.

188 *Id*. Véase también Informe de 2014 del Consejo de Derechos Humanos, *supra,* nota 45, párr. 40 (donde se destaca la importancia de la notificación y la legitimación para impugnar la vigilancia “para determinar el acceso a un recurso efectivo”).

189 TEDH, Roman Zakharov, App. No. 47143/06, *supra,* nota 39, párr. 234. Véase también TEDH, Big Brother Watch, App. No. 58170/13, *supra,* nota 123, párr. 357.

190 Véase, por ejemplo, CIDH, Informe No. 57/19, *supra,* nota 3, párr. 131- 159.

191 TEDH, Szabo, App. No. 37138/14, *supra*, nota 128, párr. 86.

192 CIDH, *Declaración de Principios sobre Libertad de Expresión*, Principio 3 (octubre de 2000), www.cidh.oas.org/Relatoria/showarticle.asp?artID=26&lID=1 [en adelante *Declaración de Principios sobre Libertad de Expresión*].

193 TJUE, Asunto C-362/14, Maximillian Schrems v. Data Protection Commissioner, ECLI:EU:C:2015:650, párr. 95 (6 de octubre de 2015) [en adelante “TJUE, Asunto C-362/14, Schrems v. Data Protection”] (donde se afirma que las leyes deben ofrecer la posibilidad “de que el justiciable ejerza acciones en Derecho para acceder a los datos personales que le conciernen o para obtener su rectificación o supresión” de conformidad con el “derecho fundamental a la tutela judicial efectiva”). Véase también Informe de 2018 del Alto Comisionado para los Derechos Humanos*, supra,* nota 51, párr. 41 (donde se señala que las personas que han sido sometidas a vigilancia tienen derecho a recibir una notificación, una explicación y la oportunidad de corregir o borrar información personal, “siempre y cuando esa información ya no sea necesaria para llevar a cabo una investigación en curso o pendiente”).

194 Véase *supra,* nota 135.

Esta Corte ha afirmado que el artículo 13 de la Convención Americana "ampara el derecho de las personas a recibir [la información que obre en poder del Estado] y la obligación positiva del Estado de suministrarla, de forma tal que la persona pueda tener acceso a conocer esa información o reciba una respuesta fundamentada cuando por algún motivo permitido por la Convención el Estado pueda limitar el acceso a la misma para el caso concreto"[195]. Reconociendo que el principio de máxima divulgación es una piedra angular de las sociedades democráticas que posibilita el escrutinio público, esta Corte ha dispuesto que los Estados están obligados a "[establecer] la presunción de que toda información es accesible, sujeto a un sistema restringido de excepciones", y ha trasladado al Estado la carga de probar que se justifica ocultar información al público[196]. No obstante, las restricciones del derecho de acceso a la información por motivos vagos y excesivamente amplios de "seguridad nacional" no son permisibles y no se encuadran en los requisitos de legalidad, legitimidad, necesidad y salvaguardias mínimas[197].

En el contexto de la vigilancia, hay un consenso internacional afianzado sobre la importancia del acceso a la información para asegurar la supervisión pública de las actividades de vigilancia del gobierno[198]. Los expertos internacionales afirman que, cuando la vigilancia es ilegal, como en este caso, "la sociedad debería ser plenamente informada" y "[l]a información acerca de este tipo de vigilancias debería ser hecha pública en la mayor medida posible, sin violar los derechos de privacidad de las personas vigiladas"[199].

2. El marco jurídico actual que regula las actividades de inteligencia en Colombia permite la vigilancia abusiva, en contravención de la Convención Americana

Colombia utiliza varias leyes internas promulgadas en la segunda década del presente siglo como argumento de que el Estado está regulando a sus órganos de inteligencia de conformidad con la Convención Americana[200]. En realidad, este marco jurídico es manifiestamente inadecuado y muy deferente con los mismos órganos que, durante decenios, han usado la vigilancia de las comunicaciones para perseguir a defensores de derechos humanos. Desde 2013, las unidades de inteligencia han seguido interceptando las comunicaciones

---

[195] Corte IDH, Caso Claude Reyes y otros vs. Chile, serie C, No. 151, *supra,* nota 87, párr. 77.

[196] *Id.*, párr. 92.

[197] Véase Informe de 2020 del Relator Especial de la CIDH para la Libertad de Expresión, *supra,* nota 164, párr. 23 (donde se critica la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional, de Colombia, porque no es suficientemente precisa); *Principios de Tshwane*, *supra,* nota 175, Principios 2 y 3; *Declaración conjunta sobre la vigilancia*, *supra,* nota 77, párr. 12.

[198] TEDH, Roman Zakharov, App. No. 47143/06, *supra,* nota 39, párr. 283 (donde se afirma que las actividades de los órganos de supervisión de la vigilancia deben estar sometidas a escrutinio público); Informe de 2020 del Relator Especial de la CIDH para la Libertad de Expresión, *supra,* nota 164, párr. 58 (donde se señala que la falta de transparencia y de acceso a la información con respecto a las actividades de vigilancia estatal crea barreras para la rendición de cuentas por el Estado); resolución 69/166 de la Asamblea General, *El derecho a la privacidad en la era digital* (18 de diciembre de 2014) (donde se exhorta a los Estados a que "[e]stablezcan o mantengan mecanismos nacionales de supervisión, de índole judicial, administrativa o parlamentaria, que cuenten con los recursos necesarios y sean independientes, efectivos e imparciales, así como capaces de asegurar la transparencia, cuando proceda, y la rendición de cuentas por las actividades de vigilancia de las comunicaciones y la interceptación y recopilación de datos personales que realice el Estado"); *Declaración conjunta sobre la vigilancia*, *supra,* nota 77, párr. 12.

[199] *Principios de Tshwane*, *supra,* nota 175, Principio 10.E.3. Véase también *Declaración conjunta sobre la vigilancia*, *supra,* nota 77, párr. 14.

[200] CIDH, Informe No. 57/19, *supra,* nota 3, párr. 28; Audiencia Pública del Caso Miembros Corporación Colectivo de Abogados CAJAR vs. Colombia Parte 2, *supra,* nota 1, 8:31:02-8:33:32.

electrónicas de miembros de la CCAJAR, actuando al margen de la ley con impunidad. La Ley de Inteligencia de 2013 no establece suficientes restricciones para los órganos de inteligencia, ya que permite el monitoreo del espectro electromagnético y el acceso a datos almacenados por proveedores de servicios de comunicaciones con fines imprecisos y de una manera indefinida, con mecanismos de supervisión inadecuados, y permite a estos órganos retener el material recopilado durante mucho tiempo. Las leyes inadecuadas en materia de protección, corrección, eliminación y transferencia de datos exacerban la vulnerabilidad de las personas sometidas a vigilancia ilegal, al privarlas de acceso a recursos. Estas leyes obstaculizan el escrutinio público con garantías anémicas de acceso del público a información sobre la vigilancia estatal de las comunicaciones. En conjunto, este marco jurídico preserva un extenso régimen de vigilancia en Colombia que opera en el sigilo y no rinde cuentas.

a. La Ley de Inteligencia da a las autoridades colombianas amplia libertad para vigilar a los defensores de derechos humanos con fines vagos y de una manera imprecisa, durante un período indefinido, sin salvaguardias adecuadas contra los abusos

Colombia no ha aseverado que la vigilancia de miembros de la CCAJAR se haya realizado en el marco de un proceso de investigación penal. Por lo tanto, el marco jurídico aplicable es la Ley de Inteligencia de 2013, que regula la vigilancia estatal *fuera* del contexto de las investigaciones penales[201]. De acuerdo con la Constitución de Colombia, se requiere una orden judicial para interceptar o registrar comunicaciones[202]. La Ley de Inteligencia, aunque no autoriza explícitamente a los órganos de inteligencia a "interceptar" comunicaciones fuera del contexto de las investigaciones penales, exime a las autoridades de inteligencia del requisito de la autorización judicial previa y de otras salvaguardias procesales para monitorear el espectro electromagnético o accesar datos almacenados por proveedores de servicios de comunicaciones. La amplitud excesiva y la vaguedad de cada una de estas actividades de vigilancia, combinadas con la falta de salvaguardias que impongan restricciones a las autoridades de inteligencia, infringen el derecho internacional de los derechos humanos y crean mucho margen para abusos.

i. La vaguedad y la amplitud excesiva de la redacción de la Ley de Inteligencia propician la vigilancia estatal ilegal

[201] Aunque el tema está fuera del alcance del presente escrito, el marco jurídico del procedimiento para la interceptación de comunicaciones en el contexto de investigaciones penales también es deficiente. De acuerdo con el artículo 15 de la Constitución de Colombia, se requiere una orden judicial para interceptar o registrar comunicaciones. CONSTITUCIÓN POLÍTICA DE COLOMBIA, art. 15, https://pdba.georgetown.edu/Constitutions/Colombia/colombia91.pdf. Sin embargo, en ciertas circunstancias, la Constitución y el Código de Procedimiento Penal permiten que el fiscal general ordene la interceptación de comunicaciones (excepto las del acusado) a efectos de una investigación penal, en cuyo caso el fiscal debe obtener una orden judicial 36 horas antes de la interceptación. *Id*., art. 250; Ley 906, art. 235 a 237, 1 de septiembre de 2004, DIARIO OFICIAL (Colombia). Esta exención de la autorización judicial previa debilita la supervisión judicial y abre la puerta a abusos de los fiscales. Véase, por ejemplo, KATITZA RODRIGUEZ, VERIDIANA ALIMONTI, NECESSARY AND PROPORTIONATE, THE STATE OF COMMUNICATION PRIVACY IN COLOMBIA 7 (2020), https://necessaryandproportionate.org/country-reports/colombia/twenty-twenty/.

[202] CONSTITUCIÓN POLÍTICA, art. 15.

En la Ley de Inteligencia no se describen con claridad los fines con los cuales los órganos de inteligencia pueden vigilar a personas por medio del monitoreo del espectro electromagnético o del acceso a datos almacenados por proveedores de servicios de comunicaciones. En el artículo 4 de la Ley hay una lista de los fines para los cuales se autorizan actividades de inteligencia y contrainteligencia, entre ellos asegurar "el régimen democrático, la integridad territorial, la soberanía, la seguridad y la defensa de la Nación", proteger al país y a su pueblo "frente a amenazas tales como el terrorismo, el crimen organizado, el narcotráfico, el secuestro, el tráfico de armas, municiones, explosivos y otros materiales relacionados, el lavado de activos [...]" y proteger "los recursos naturales y los intereses económicos de la Nación"[203]. En la Ley no se explica qué podría constituir una amenaza —por ejemplo, una "amenaza para la seguridad nacional"— que justifique la vigilancia.

Mientras que el Tribunal Europeo de Derechos Humanos ha determinado que la "seguridad nacional" es una justificación suficientemente precisa para la vigilancia[204], el Relator Especial de la CIDH para la Libertad de Expresión y otros expertos en derechos humanos han formulado advertencias con respecto a tal grado de imprecisión, ya que "las razones de seguridad nacional suelen ser invocadas para poner bajo vigilancia a defensores de derechos humanos, periodistas, comunicadores o activistas"[205]. Esta Corte debe tener en cuenta el contexto de América Latina en general y de Colombia en particular y rechazar el enfoque peligrosamente permisivo adoptado por el Tribunal Europeo. Como observa la Comisión Interamericana en su informe de fondo, varios funcionarios públicos colombianos, entre ellos el expresidente Álvaro Uribe Vélez, han usado de manera sistemática el pretexto de la seguridad nacional para calificar de amenazas a defensores de derechos humanos, entre ellos miembros de la CCAJAR[206]. Los órganos de inteligencia colombianos también han usado esto como estrategia básica para suprimir la disidencia del público[207].

Esta Corte ha reconocido en reiteradas ocasiones las consecuencias catastróficas del pretexto de la seguridad nacional utilizado por los Estados y del concepto de "enemigo interno" para perseguir a civiles, en particular defensores de derechos humanos, en Colombia[208] y en otros países de América Latina[209]. El otorgamiento de amplias facultades discrecionales a los órganos de inteligencia, sin mayor orientación en la ley, para determinar qué podría constituir una amenaza para el régimen y para la seguridad nacional, pone en peligro a los defensores de derechos humanos en Colombia. La Corte no debe consentir un enfoque tan peligroso.

---

[203] Ley 1621, art. 4, 17 de abril de 2013, DIARIO OFICIAL (Colombia) [en adelante "Ley de Inteligencia de 2013"].

[204] TEDH, Big Brother Watch, App. No. 58170/13, *supra,* nota 123, párr. 365 (donde se señala que el Tribunal Europeo de Derechos Humanos considera que el régimen perseguía el fin legítimo de proteger la seguridad nacional).

[205] Informe de 2013 de la Relatora Especial de la CIDH para la Libertad de Expresión, *supra,* nota 78, párr. 158. Véase también Informe de 2018 del Alto Comisionado para los Derechos Humanos, *supra,* nota 51, párr. 35 (donde dice que "[l]as justificaciones imprecisas y excesivamente amplias, como las referencias vagas a la 'seguridad nacional', no pueden considerarse disposiciones suficientemente claras").

[206] CIDH, Informe No. 57/19, *supra,* nota 3, párrs. 64 y 171.

[207] *Id.*, párr. 135 (donde se observa que el Grupo Especial de Inteligencia G-3 trabajó en "el seguimiento a organizaciones y personas de tendencia opositora frente a las políticas gubernamentales [...] a efectos de 'restringir o neutralizar su accionar'").

[208] Véase, por ejemplo, Corte IDH, Villamizar Durán y otros vs. Colombia, serie C, No. 364*, supra,* nota 140, párrs. 64 y 65; Corte IDH, Caso Isaza Uribe y otros vs. Colombia, serie C, No. 363*, supra,* nota 140, párrs. 127 y 128. Asimismo, esta Corte ha determinado que un elemento indispensable para la transición de Colombia a la paz es una mayor transparencia con respecto a los parámetros de la doctrina de seguridad nacional. *Id*., párr. 207.

[209] Véase *supra,* nota 140.

ii. La Ley de Inteligencia no ha prevenido la interceptación ilegal de comunicaciones por órganos de inteligencia

La Ley de Inteligencia de 2013 no ha impedido que los órganos de inteligencia colombianos "intercepten" comunicaciones, actividad que no está autorizada en el derecho colombiano fuera del ámbito de las investigaciones penales. La Constitución prohíbe la "interceptación" de comunicaciones privadas sin orden judicial[210]. El Código de Procedimiento Penal permite que las autoridades de las fuerzas del orden "intercepten" comunicaciones en el curso de investigaciones penales, mientras que la Ley de Inteligencia autoriza a los órganos de inteligencia a realizar otros tipos de vigilancia, como monitoreo del espectro electromagnético y acceso a información y metadatos de los abonados almacenados por proveedores de servicios de comunicaciones[211]. De acuerdo con la Ley de Inteligencia, el monitoreo del espectro electromagnético es diferente de la "interceptación de conversaciones privadas telefónicas móviles o fijas, así como de las comunicaciones privadas de datos", que no está autorizada por la Ley de Inteligencia, sino que "deberán someterse a los requisitos establecidos en el artículo 15 de la Constitución y el Código de Procedimiento Penal y sólo podrán llevarse a cabo en el marco de procedimientos judiciales"[212]. En términos sencillos, la Ley de Inteligencia no autoriza a los órganos de inteligencia a "interceptar" comunicaciones privadas.

No obstante, las afirmaciones realizadas durante la audiencia pública indican que las comunicaciones de defensores de derechos humanos, entre ellos la CCAJAR, de hecho han sido interceptadas desde 2013, año en que se promulgó la Ley de Inteligencia[213]. Como en las leyes colombianas no se autoriza a los órganos de inteligencia a interceptar comunicaciones, estos actos no se fundamentan en el derecho y, por consiguiente, infringen el principio de legalidad, según el cual toda injerencia en los derechos humanos causada por la vigilancia que se realice debe "estar prevista en ley" y se prohíbe que los Estados causen injerencias en un caso que no esté "previsto" por ley[214].

Esta realidad también contradice las declaraciones de Colombia de que "establece de manera clara y precisa las circunstancias concretas en que [las labores de inteligencia] pueden ser autorizadas para garantizar que toda actuación se ajuste a los principios de legalidad, proporcionalidad y necesidad"[215]. En la Ley de Inteligencia no se explica con claridad en qué consiste el "monitoreo del espectro electromagnético"; simplemente se señala que no se le aplican los requisitos del artículo 15 de la Constitución porque —según declara la Ley en beneficio propio— "[e]l monitoreo no constituye interceptación de comunicaciones"[216].

---

210 CONSTITUCIÓN POLÍTICA, art. 15.

211 Ley de Inteligencia de 2013, *supra,* nota 203, arts. 17 y 44.

212 *Id.*, art. 17. Como ya se ha señalado, los procedimientos para interceptar comunicaciones en el contexto de investigaciones penales, que se establecen en el artículo 250 de la Constitución y en los artículos 235 a 237 del Código de Procedimiento Penal, también son deficientes. Véase *supra,* nota 201.

213 Véase, Audiencia Pública del Caso Miembros Corporación Colectivo de Abogados CAJAR vs. Colombia Parte 2, *supra,* nota 1, 7:52:30-7:59:53.

214 Corte IDH, Caso Tristán Donoso vs. Panamá, serie C, No. 193, *supra,* nota 122, párrs. 76 y 80.

215 Audiencia Pública del Caso Miembros Corporación Colectivo de Abogados CAJAR vs. Colombia Parte 2, *supra,* nota 1, 8:32:28-8:32:49.

216 Ley de Inteligencia de 2013, *supra,* nota 203, art. 17.

En la Ley de Inteligencia no se define la expresión "monitoreo del espectro electromagnético" ni se indica qué tecnología se usaría para efectuarlo, cómo difiere de la "interceptación" o cómo se podría evitar la injerencia en las comunicaciones privadas. Ante la falta de una definición clara, el Comité de Derechos Humanos ha expresado la preocupación de que, en el desarrollo del monitoreo del espectro electromagnético con arreglo a la Ley de Inteligencia, "pudieran presentarse en la práctica injerencias en las comunicaciones privadas realizadas a través del espectro electromagnético que no estén sujetas a una estricta evaluación de legalidad, necesidad y proporcionalidad"[217].

En 2012, al examinar la validez constitucional de esta disposición, la Corte Constitucional de Colombia entendió que el monitoreo del espectro electromagnético es un actividad que "consiste en llevar a cabo una labor de rastreo de forma aleatoria e *indiscriminada*. Ello implica la *captación incidental de comunicaciones en las que se revelan circunstancias* que permiten evitar atentados y controlar riesgos para la defensa y seguridad de la Nación. Técnicamente se estaría ante una especie de rastreo de sombras, imágenes y sonidos representados en frecuencias de radiación electromagnética y ondas radioeléctricas"[218]. La Corte Constitucional, a pesar de que reconoció que el monitoreo del espectro electromagnético "implica la captación incidental de comunicaciones en las que se revelan circunstancias", llegó a la conclusión incongruente de que el monitoreo del espectro electromagnético "no puede implicar interceptación o registro de las comunicaciones privadas, toda vez que para ello se requiere *'orden judicial, en los casos y con las formalidades que establezca la ley'*. [...] Por tanto, el monitoreo del espectro electromagnético es una actividad limitada por los derechos fundamentales y sujeta al sistema de control de poderes establecido en la Constitución [...], que no pueden ser vulnerados so pretexto del adelantamiento de tal actividad"[219].

Esta Corte debe tener en cuenta que la Corte Constitucional de Colombia emitió este fallo en 2012, antes de las revelaciones efectuadas por Edward Snowden en 2013 con respecto al abuso generalizado por el estado de la vigilancia masiva y los medios de obtención de inteligencia en Estados Unidos y en otros lugares. Estas revelaciones llevaron a los órganos de derechos humanos a desarollar normas que constituyen la base actual de la jurisprudencia internacional de derechos humanos en materia de inteligencia y vigilancia[220]. Estas normas aclaran que la captación indiscriminada y a menudo "incidental" de comunicaciones constituye una injerencia desproporcionada en los derechos humanos[221]. Según el derecho internacional de

---

[217] Comité de Derechos Humanos, *Observaciones finales sobre el séptimo informe periódico de Colombia*, párr. 32, U.N. Doc. CCPR/C/COL/CO/7 (17 de noviembre de 2016). Véase también ACNUDH, *Informe anual del Alto Comisionado de las Naciones Unidas para los Derechos Humanos sobre la situación de los derechos humanos en Colombia*, párr. 84, U.N. Doc. A/HRC/34/3/Add.3 (14 de marzo de 2017) [en adelante "Informe del ACNUDH de 2017 sobre Colombia"] (donde se recalca que, "para garantizar la legalidad, proporcionalidad y necesidad de la recopilación de datos sobre personas y la aceptación pública de la facultad de vigilar el espectro electromagnético prevista en la Ley de Inteligencia [...], el Gobierno debe aclarar el alcance y la regulación de esa facultad").

[218] Corte Constitucional, 12 de julio de 2012, Sentencia C-540/12, párr. 3.9.17.2.3, Gaceta de la Corte Constitucional (Colombia) (énfasis añadido). Véase también Comité de Derechos Humanos, *Lista de cuestiones relativa al séptimo informe periódico de Colombia. Adición. Respuestas de Colombia a la lista de cuestiones*, párrs. 95 y 96, U.N. Doc. CCPR/C/COL/Q/7/Add.1 (18 de agosto de 2016).

[219] Corte Constitucional, Sentencia C-540/12, *supra,* nota 218, párr. 3.9.17.2.3.

[220] Véase, por ejemplo, TEDH, Big Brother Watch, App. No. 58170/13, *supra,* nota 123, párr. 8 (opinión en parte concordante y en parte discordante del juez, en la cual se describe la plétora de documentos convincentes sobre la interceptación a gran escala publicados por el Consejo de Europa, la Unión Europea, el Comité de Derechos Humanos y otros expertos internacionales en la materia tras el estallido del escándalo Snowden).

[221] Véase *supra*, notas 148 a 155.

los derechos humanos, se deben aplicar las mismas protecciones a todos los datos, incluidos los metadatos[222]. La Corte Constitucional de Colombia simplemente no tenía en ese momento la posibilidad de recurrir al consenso internacional surgido después de 2013, que la Corte Interamericana debe tener en cuenta en la actualidad.

De todas maneras, el razonamiento de la Corte Constitucional es circular (al dictaminar que el monitoreo no es interceptación porque simplemente no puede serlo de acuerdo con la Constitución) e inviable. Por el espectro electromagnético se encaminan diversas ondas, entre ellas ondas radioeléctricas que se usan para transmitir comunicaciones entre dispositivos electrónicos, como wifi[223]. El monitoreo del espectro electromagnético puede implicar la captación, el registro, el procesamiento y la evaluación de estas ondas[224]. Privacy International ya ha señalado lo siguiente:

> Aunque se pueda afirmar que existen medios para "monitorear" el espectro electromagnético sin violar la intimidad de las comunicaciones, estos medios corresponden a un conjunto extremadamente limitado de actividades, como las que se realizan con herramientas de detección de calor y herramientas y antenas de localización de dirección. Las demás formas de "monitoreo" del espectro electromagnético implican un tipo de injerencia en una comunicación del cual solo se puede inferir que el monitoreo ha resultado en la interceptación de la comunicación[225].

Ni en la Ley de Inteligencia ni en la argumentación de la Corte Constitucional se define en medida suficiente la forma en que Colombia podrá monitorear el espectro electromagnético con la garantía de que no haya injerencias en las comunicaciones privadas. De hecho, la propia Corte Constitucional observa que el monitoreo del espectro electromagnético podría implicar "la captación incidental de comunicaciones"[226], con lo cual no impide que las autoridades de inteligencia colombianas clasifiquen una amplia gama de actividades de vigilancia como monitoreo del espectro electromagnético para evitar la salvaguardia procesal requerida de conformidad con el artículo 15 de la Constitución.

iii. La Ley de Inteligencia confiere a las autoridades de inteligencia facultades imprecisas para tener acceso a metadatos almacenados por proveedores de servicios de comunicaciones, en contravención del principio de proporcionalidad

Además de permitir el monitoreo del espectro electromagnético, la Ley de Inteligencia confiere a las autoridades facultades imprecisas para tener acceso a datos de las comunicaciones —"metadatos"— almacenados por proveedores de servicios de comunicaciones. De acuerdo con el artículo 44 de la Ley de Inteligencia, las autoridades están facultadas para obtener "el historial de comunicaciones de los abonados telefónicos vinculados, los datos técnicos de identificación

---

222 Véase *infra*, nota 230.

223 Congressional Research Service, *Overview of Department of Defense Use of the Electromagnetic Spectrum* 2 (2021), https://crsreports.congress.gov/product/pdf/R/R46564/8.

224 Ali Boyacı et al., *Monitoring, Surveillance, and Management of the Electromagnetic Spectrum: Current Issues in Electromagnetic Spectrum Monitoring*, 18 ELECTRICA 100, 101 (2018), https://electricajournal.org/Content/files/sayilar/28/100-108.pdf.

225 PRIVACY INTERNATIONAL, THE RIGHT TO PRIVACY IN COLOMBIA, 5, n. 13 (2016), https://privacyinternational.org/sites/default/files/2017-12/HRC_colombia.pdf. Traducción de International Human Rights Law Clinic.

226 Corte Constitucional, Sentencia C-540/12, *supra,* nota 218, párr. 3.9.17.2.3.

de los suscriptores [...], así como la localización de las celdas en que se encuentran la terminales y cualquier otra información que contribuya a su localización"[227]. El director del órgano de inteligencia está facultado para presentar la solicitud correspondiente[228]. En la Ley de Inteligencia no se definen de manera clara o precisa los datos abarcados por "el historial de comunicaciones" o "los datos técnicos de identificación de los suscriptores"[229]. Igual que lo hace en relación con el monitoreo del espectro electromagnético, el artículo 44 de la Ley de Inteligencia señala que "la interceptación de comunicaciones estará sujeta a los procedimientos establecidos por el artículo 15 de la Constitución y el Código de Procedimiento Penal". Sin embargo, esta distinción entre "interceptación" de comunicaciones y adquisición de metadatos no encuentra fundamento en el derecho internacional de los derechos humanos. Tras la promulgación de la Ley de Inteligencia ha surgido un consenso internacional generalizado en lo que respecta al reconocimiento de que los metadatos contienen información que es tan delicada como la contenida en las comunicaciones y que el acceso de órganos de inteligencia a los metadatos constituye una injerencia en los derechos humanos[230]. Al conferir a los órganos de inteligencia facultades imprecisas para acceder a metadatos al margen de las salvaguardias de la Constitución, la Ley de Inteligencia es violatoria de los principios de necesidad y proporcionalidad.

iv. La Ley de Inteligencia no limita debidamente quiénes pueden ser objeto de vigilancia de las comunicaciones

En la Ley de Inteligencia no se indica qué relación debe existir entre las amenazas enumeradas que justifican las actividades de inteligencia, incluido el monitoreo del espectro electromagnético y el acceso a metadatos almacenados por proveedores de servicios de comunicaciones, y *las personas* que pueden ser objeto de dichas actividades[231]. Además, la Corte Constitucional ha entendido que el monitoreo del espectro electromagnético implica "una labor

---

227 Ley de Inteligencia de 2013, *supra,* nota 203, art. 44.

228 *Id.*

229 FUNDACIÓN KARISMA, UN RASTREADOR EN TU BOLSILLO: ANÁLISIS DEL SISTEMA DE REGISTRO DE CELULARES EN COLOMBIA 27 (2017), https://nomascelusvigilados.karisma.org.co/para-leer/informe-de-investigaci%C3%B3n.html.

230 Véase Corte IDH, Caso Escher y otros vs. Brasil, serie C, No. 200, *supra,* nota 44, párr. 114 (donde se señala que las medidas de protección se extienden a "cualquier otro elemento del proceso comunicativo mismo, por ejemplo, el destino de las llamadas que salen o el origen de las que ingresan, la identidad de los interlocutores, la frecuencia, hora y duración de las llamadas"); CIDH, *Estándares para Internet del Relator Especial de la CIDH para la Libertad de Expresión*, *supra,* nota 54, párr. 189 (donde se explica que los metadatos, "al igual que los datos relativos a las comunicaciones telefónicas, protegidos por la jurisprudencia del sistema interamericano, son distintos del contenido pero son altamente reveladores de relaciones personales, hábitos y costumbres, gustos, estilos y formas de vida, etc."); TEDH, Big Brother Watch, App. No. 58170/13, *supra,* nota 123, párr. 363 (donde se señala que el Tribunal Europeo de Derechos Humanos no está convencido de que la adquisición de datos relacionados de las comunicaciones por medio de la interceptación a gran escala sea necesariamente menos intrusiva que la adquisición de contenido. Por lo tanto, el Tribunal considera que la interceptación, la retención y la búsqueda de datos relacionados de las comunicaciones deberían analizarse por referencia a las mismas salvaguardias que se aplican al contenido); TJUE, Asuntos acumulados C-203/15 y C-698/15, Tele2 v. Post-och, *supra,* nota 82, párr. 99 (donde se afirma que los metadatos, "considerados en su conjunto, permiten extraer conclusiones muy precisas sobre la vida privada de las personas cuyos datos se han conservado, como los hábitos de la vida cotidiana, los lugares de residencia permanentes o temporales, los desplazamientos diarios u otros, las actividades realizadas, sus relaciones sociales y los círculos sociales que frecuentan [...]. En particular, estos datos proporcionan medios para determinar [...] el perfil de las personas afectadas, información tan sensible, a la luz del respeto de la vida privada, como el propio contenido de las comunicaciones"); *Observaciones finales del Comité de Derechos Humanos sobre Estados Unidos*, *supra,* nota 39, párr. 22 (donde se expresa preocupación por los efectos adversos que tiene en el derecho a la privacidad la recopilación de metadatos y contenido de comunicaciones); Informe de 2018 del Alto Comisionado para los Derechos Humanos, *supra,* nota 51, párr. 6; resolución 69/166 de la Asamblea General, *supra,* nota 198, párr. 2.

231 TEDH, Szabo, App. No. 37138/14, *supra,* nota 128, párr. 67.

de rastreo de forma aleatoria e indiscriminada" y "la captación incidental de comunicaciones"[232]. Eso no proporciona suficiente orientación y crea el riesgo de permitir la vigilancia de una amplia categoría de personas, muchas de las cuales podrían estar conectadas de manera tangencial a la presunta amenaza y muchas más posiblemente no estén conectadas en absoluto. La Comisión Interamericana, el Tribunal de Justicia de la Unión Europea, el Comité de Derechos Humanos y los expertos de las Naciones Unidas en la materia han afirmado que la vigilancia masiva indiscriminada, incluido el acceso a metadatos almacenados por proveedores de servicios de comunicaciones, no es permisible de acuerdo con el derecho internacional de los derechos humanos[233]. Asimismo, en el contexto de la vigilancia interna, el Tribunal Europeo de Derechos Humanos ha expresado acuerdo con este consenso internacional[234]. Aunque lo ha contradicho al permitir la interceptación masiva de comunicaciones extranjeras, ha continuado recalcando la importancia de establecer *ciertos* límites con respecto a quiénes pueden ser vigilados[235].

v. La Ley de Inteligencia no indica de forma clara la duración permitida de la vigilancia y posibilita la retención de datos durante períodos excesivamente largos

Contrariamente al requisito de que en las leyes se defina de manera precisa la duración de la vigilancia y el tiempo durante el cual se puede retener el material recopilado[236], en la Ley de Inteligencia no se aclara ninguno de estos dos aspectos, en contravención de los principios de necesidad y proporcionalidad. El Tribunal Europeo de Derechos Humanos ha observado que el almacenamiento de material sobre la vida privada de una persona constituye de por sí una injerencia en el derecho a la privacidad y, por consiguiente, debe estar limitado por los principios de necesidad y proporcionalidad[237]. Además, el Tribunal y expertos en derechos humanos de Europa, las Américas, África y las Naciones Unidas están de acuerdo en que la duración de la retención también debe ser limitada de acuerdo con los principios de necesidad y proporcionalidad[238]. En la Ley de Inteligencia de Colombia no se limita de manera apropiada el

[232] Corte Constitucional, Sentencia C-540/12, *supra,* nota 218, párr. 3.9.17.2.3.
[233] Véase *supra*, notas 148 a 155.
[234] TEDH, Szabo, App. No. 37138/14, *supra,* nota 128, párr. 67 (donde se expresa grave preocupación porque en la legislación interna no se requiere que haya una conexión entre la persona que será vigilada y la amenaza. Por consiguiente, se permitió la vigilancia de realmente cualquier persona, lo cual no es permisible, y se allanó el camino para la vigilancia ilimitada de un gran número de ciudadanos por razones de seguridad nacional); TEDH, Roman Zakharov, App. No. 47143/06, *supra,* nota 39, párr. 265 (donde se concluye que la ley de inteligencia era inadecuada, en parte porque no contenía ningún requisito con respecto al contenido de la solicitud de interceptación ni al contenido de la autorización de la interceptación. En consecuencia, los tribunales a veces otorgan permisos de interceptación en los cuales no se menciona una persona en particular ni el número telefónico que será intervenido, sino que se autoriza la interceptación de todas las comunicaciones telefónicas de la zona donde se ha cometido un delito).
[235] Véase, por ejemplo, TEDH, Big Brother Watch, App. No. 58170/13, *supra,* nota 123, párr. 375 (donde se señala que el régimen de vigilancia a gran escala del Reino Unido se aplicaba solo a las comunicaciones enviadas o recibidas fuera del Reino Unido y se restringían, aunque de forma limitada, las categorías de personas cuyas comunicaciones podían interceptarse).
[236] Véase, por ejemplo, TEDH, Ekimdzhiev, App. No. 70078/12, *supra,* nota 120, párr. 305 (donde se afirma que, aunque en las leyes búlgaras se indica claramente la duración máxima permitida de la vigilancia, la restricción es insuficiente debido a la duración misma de ese período, que es de dos años); *id*., párr. 329 (en las leyes búlgaras no se indicaba de una manera suficientemente clara la forma en que se destruiría el material probatorio obtenido por medio de la vigilancia); *Joint Declaration on Freedom of Expression*, *supra,* nota 149, párr. 8.b.
[237] TEDH, Rotaru v. Romania, *supra*, nota 82, párrs. 46 a 48 (4 de mayo de 2000).
[238] Véase TEDH, Big Brother Watch, App. No. 58170/13, *supra,* nota 123, párr. 422 (donde se examina la duración del almacenamiento del material retenido); *Joint Declaration on Freedom of Expression*, *supra,* nota 149, párr. 8.b.

tiempo que los organismos pueden retener el material recopilado[239]. La Ley permite que los organismos mantengan esos materiales clasificados durante treinta (30) años, plazo que solo el presidente puede prorrogar otros quince (15) años, sin la clara supervisión de una autoridad independiente[240]. En la Ley de Inteligencia tampoco se limita con claridad la duración de la vigilancia.

Por último, además de la retención de los datos recopilados por órganos de inteligencia, en las leyes colombianas también se prevé la conservación indiscriminada de metadatos por terceros proveedores de servicios de comunicaciones durante largos períodos. De acuerdo con el artículo 44 de la Ley de Inteligencia, las autoridades de inteligencia pueden solicitar metadatos de proveedores de servicios de comunicaciones durante un plazo de cinco años. Además, según el artículo 4 del Decreto 1704 de 2012 sobre reglamentación de las telecomunicaciones, los proveedores de servicios de telecomunicaciones deben mantener actualizada la información de sus suscriptores —como identidad, dirección de facturación y tipo de conexión— y conservarla durante cinco años como mínimo[241]. El artículo 5 del Decreto requiere que, en asuntos penales, los proveedores suministren a la Fiscalía General información "tal como sectores, coordenadas geográficas y potencia, entre otras, que contribuya a determinar la ubicación geográfica de los equipos terminales o dispositivos que intervienen en la comunicación"[242]. Por último, en virtud de la Resolución 912 de 2008, los proveedores de servicios de comunicaciones deben permitir el acceso de la Dirección de Investigación Criminal (Dijin) de la Policía Nacional a información de los usuarios, como nombre y número de identificación, domicilio y fecha de activación[243]. En conjunto, estas leyes requieren que los proveedores de servicios de comunicaciones conserven una amplia gama de metadatos —entre ellos información sobre la identidad de los usuarios, geolocalización e historial de comunicaciones— a los cuales las autoridades de inteligencia pueden tener acceso durante un período de hasta cinco años.

La retención masiva e indiscriminada de metadatos constituye una infracción desproporcionada del derecho a la privacidad[244]. En 2014, el Tribunal de Justicia de la Unión Europea examinó la compatibilidad de una directiva de la Unión Europea sobre la retención de metadatos con la Carta de los Derechos Fundamentales de la Unión Europea, específicamente en lo que se refiere al respeto de la vida privada[245]. El Tribunal afirmó que la directiva era incompatible con el principio de necesidad porque requería la retención masiva e indiscriminada de metadatos y no establecía restricciones para el período durante el cual debían conservarse esos

---

[239] Ley de Inteligencia de 2013, *supra,* nota 203, art. 33. TEDH, Big Brother Watch, App. No. 58170/13, *supra,* nota 123, párr. 403 (donde se concluye que el régimen de vigilancia del Reino Unido es adecuado porque, en general, el material se borra al cabo de unos meses, pero se señala que habría sido conveniente que, en la legislación, se hubiera indicado este período de retención más corto, en vez del período máximo de dos años).

[240] El Relator Especial de la CIDH para la Libertad de Expresión ha criticado esta disposición de la ley porque es ambigua y desproporcionada, ya que permite a las autoridades de inteligencia clasificar todos sus documentos como secretos sin tener en cuenta su contenido y sin un procedimiento claro o adecuado para la clasificación. Informe de 2020 del Relator Especial de la CIDH para la Libertad de Expresión, *supra,* nota 164, párrs. 25 a 27.

[241] Decreto 1704, art. 4, 15 de agosto de 2012, DIARIO OFICIAL (Colombia).

[242] *Id.*, art. 5.

[243] Resolución 912 de 2008 Por la cual se reglamenta el suministro de información de suscriptores y usuarios autorizados para el uso de las telecomunicaciones al igual que las redes de los concesionarios y licenciatarios, 15 de enero de 2009, DIARIO OFICIAL (Colombia).

[244] Como ya se ha señalado, hay consenso internacional en que la injerencia en los metadatos es tan intrusiva como la injerencia en el contenido de las comunicaciones. Véase *supra,* nota 230.

[245] TJUE, Asunto C-293/12, DRI v. Minister, *supra,* nota 144, párr. 18.

datos, entre otras limitaciones[246], y especificó que, de una manera que no era permisible, la directiva de la Unión Europea requería la conservación de metadatos durante un período mínimo de seis meses y de 24 meses como máximo, pero no establecía ninguna distinción entre las categorías de metadatos retenidos según su utilidad ni establecía criterios objetivos para determinar cuánto tiempo (entre seis meses y 24 meses) debían conservarse determinados metadatos[247]. Análogamente, el Comité de Derechos Humanos ha dictaminado que las políticas en materia de retención de datos constituyen una injerencia en el derecho a la privacidad y que, como regla general, los Estados deben "[a]bstenerse de imponer la retención obligatoria de datos por terceros"[248]. Al requerir la retención masiva e indiscriminada de metadatos de toda la población colombiana y al no establecer ningún criterio para limitar el tipo de datos conservados, las leyes colombianas son violatorias de los principios de necesidad y proporcionalidad.

vi. La Ley de Inteligencia exime a los órganos de inteligencia de todo proceso significativo de autorización, supervisión o notificación, lo cual exacerba las amenazas planteadas por las excesivas facultades discrecionales otorgadas a estos órganos

La falta de salvaguardias significativas para evitar los abusos exacerba las excesivas facultades discrecionales que la Ley de Inteligencia otorga a las autoridades de inteligencia para determinar quién puede realizar labores de vigilancia, por qué, de quién y de qué forma. Los órganos de inteligencia hacen caso omiso sistemáticamente de las salvaguardias, y la ley exime de autorización judicial previa a ciertas actividades de vigilancia (monitoreo del espectro electromagnético y acceso a datos almacenados por proveedores de servicios de comunicaciones) realizadas por autoridades de inteligencia, no establece mecanismos adecuados de supervisión de las autoridades de inteligencia y promueve el sigilo y la falta de rendición de cuentas al omitir el requisito de la notificación.

El procedimiento establecido en la Ley de Inteligencia para las actividades en este ámbito es peligrosamente inadecuado. De conformidad con el artículo 14 de la Ley:

> Las actividades de inteligencia y contrainteligencia deberán ser autorizadas por orden de operaciones o misión de trabajo emitida por los directores de los organismos, o jefes o subjefes de unidad, sección o dependencia, según el equivalente en cada organismo, y deberán incluir un planeamiento.
>
> El nivel de autorización requerido para cada operación o misión de trabajo se incrementará dependiendo de su naturaleza y posible impacto, el tipo de objetivo, el nivel de riesgo para las fuentes o los agentes, y la posible limitación de los derechos fundamentales. Cada organismo definirá, de conformidad con su estructura interna y atendiendo los criterios establecidos en este artículo, quién es el jefe o subjefe de

[246] *Id.*, párrs. 56 a 59. Pero véase Asuntos acumulados C-511/18, C-512/18 y C-520/18, La Quadrature du Net, *supra,* nota 151, párr. 139 (donde se señala que los Estados pueden requerir que los proveedores de servicios de comunicaciones retengan de manera indiscriminada ciertos datos de las comunicaciones con fines de seguridad nacional solo si se aplican salvaguardias estrictas, entre ellas la revisión por una autoridad independiente).

[247] TJUE, Asunto C-293/12, DRI v. Minister, *supra,* nota 144, párr. 63.

[248] *Observaciones finales del Comité de Derechos Humanos sobre Estados Unidos*, *supra,* nota 39, párr. 22.d. Informe de 2014 del Alto Comisionado para los Derechos Humanos, *supra,* nota 45, párr. 26 (donde dice: "La conservación obligatoria de datos de terceros —característica frecuente de los regímenes de vigilancia de muchos Estados, cuyos gobiernos exigen a las compañías telefónicas y a los proveedores de servicios de Internet que almacenen los metadatos acerca de las comunicaciones y la ubicación de sus clientes para que las fuerzas del orden y los organismos de inteligencia puedan acceder posteriormente a ellos— no parece necesaria ni proporcionada").

> unidad, sección o dependencia encargado de la autorización, en cada caso teniendo en cuenta la Constitución y la Ley[249].

Asimismo, con respecto al acceso de los órganos de inteligencia a metadatos conservados por proveedores de servicios de comunicaciones, el artículo 44 de la Ley dice simplemente: "Los Directores de los organismos de inteligencia, o quienes ellos deleguen, serán los encargados de presentar por escrito a los operadores de servicios de telecomunicaciones la solicitud de dicha información"[250].

Estos procedimientos son enteramente internos y no exigen que una autoridad ajena al órgano de inteligencia autorice la realización de actividades de vigilancia por estos órganos, entre ellas el monitoreo del espectro electromagnético y el acceso a datos almacenados por proveedores de servicios de comunicaciones. En cambio, cada órgano determina por sí mismo el nivel de autorización requerido, según, por ejemplo, su propia valoración del grado en que una medida podría limitar derechos fundamental. En ningún momento se exige que un ente judicial apruebe las actividades de vigilancia realizadas por órganos de inteligencia.

En lo que se refiere al acceso al contenido de las comunicaciones, en el caso Szabo contra Hungría, el Tribunal Europeo de Derechos Humanos examinó la validez de un proceso de autorización que requería que el órgano de inteligencia, subordinado al Ministerio del Interior, solicitara la autorización del Ministerio de Justicia. El Tribunal afirmó que el proceso era inadecuado, ya que la supervisión a cargo de un miembro responsable del Poder Ejecutivo, como el Ministerio de Justicia, no ofrecía las garantías necesarias[251]. En cuanto al acceso a metadatos, en el caso Digital Rights Ireland contra el Reino Unido, el Tribunal de Justicia de la Unión Europea determinó que la directiva de la Unión Europea sobre conservación de metadatos no ofrecía suficiente protección contra abusos porque "el acceso a los datos conservados por las autoridades nacionales competentes no se supedita a un control previo efectuado, bien por un órgano jurisdiccional, bien por un organismo administrativo autónomo"[252].

La Ley de Inteligencia tampoco proporciona ninguna orientación instructiva sobre el contenido de las autorizaciones. El artículo 15 simplemente indica al superior jerárquico los fines enunciados de manera vaga en el artículo 4, los principios de las actividades de inteligencia previstos en el artículo 5 (donde se enumeran los principios de necesidad, idoneidad y proporcionalidad) y un "programa de planeamiento" que debe ser formulado por las autoridades de inteligencia[253]. No se requiere que la autoridad solicitante presente una solicitud fundamentada. Tampoco se requiere que la autoridad que confiere la autorización indique si la medida de vigilancia se ciñe a los principios de legalidad, legitimidad, necesidad y

---

[249] Ley de Inteligencia de 2013, *supra,* nota 203, art. 14.

[250] *Id.* art. 44.

[251] TEDH*,* Szabo, App. No. 37138/14, *supra,* nota 128, párr. 77. Véase también TEDH, Roman Zakharov, App. No. 47143/06, *supra,* nota 39, párrs. 258 y 259 (donde se señala que la autorización de la intervención de líneas telefónicas por una autoridad no judicial podría ser compatible con la Convención siempre que dicha autoridad sea suficientemente independiente del Poder Ejecutivo).

[252] TJUE, Asunto C-293/12, DRI v. Minister, *supra,* nota 144, párr. 62. Véase también TJUE, Asunto C-746/18, H. K. v. Prokuratuur, ECLI:EU:C:2021:152, párrs. 26 y 59 (2 de marzo de 2021) (donde se afirma que el "Ministerio Fiscal —cuya función es dirigir el procedimiento de instrucción penal y ejercer, en su caso, la acusación pública en un procedimiento posterior—" no era un organismo suficientemente independiente "para autorizar el acceso de una autoridad pública a los datos de tráfico y de localización a efectos de la instrucción penal").

[253] Ley de Inteligencia de 2013, *supra,* nota 203, art. 15.

proporcionalidad y de qué forma ni que señale en su autorización a quién o qué se vigilará y durante cuánto tiempo. Desprovista de estos requisitos, la Ley no asegura que las medidas de vigilancia adoptadas con arreglo a ella sean compatibles con la jurisprudencia interamericana[254].

Además de las lagunas que presenta en el proceso de autorización, la Ley de Inteligencia carece de un mecanismo de supervisión independiente. En los artículos 18 a 26 se dispone la forma en que deben supervisarse las actividades de inteligencia. De acuerdo con el artículo 18, los órganos de inteligencia deben rendir un informe anual de carácter reservado para verificar lo siguiente:

> ... la aplicación de los principios, límites y fines enunciados en esta Ley en la autorización y el desarrollo de actividades de inteligencia y contrainteligencia; la adecuación de la doctrina, los procedimientos y métodos de inteligencia a lo establecido en la presente Ley; así como la verificación de los procesos de actualización, corrección y retiro de datos y archivos de inteligencia y contrainteligencia[255].

Los órganos de inteligencia deben presentar este informe al Ministro de Defensa, a la Comisión Legal de Seguimiento a las Actividades de Inteligencia y Contrainteligencia ("Comisión Legal") y, en algunos casos, directamente al presidente[256]. Los agentes de inteligencia deben comunicar toda irregularidad al jefe del órgano de inteligencia o al "Jefe de la Oficina de Control Interno"[257]. El Ministro de Defensa y el presidente forman parte del Poder Ejecutivo y, por lo tanto, no son independientes. Tampoco lo son, por supuesto, el jefe del órgano de inteligencia ni el jefe de la oficina de control interno de dicho órgano.

Aunque la Comisión Legal es en verdad un órgano externo integrado por ocho miembros del Congreso (cuatro senadores y cuatro representantes)[258], sus facultades de supervisión son muy limitadas y no constituyen una supervisión válida. La Ley de Inteligencia autoriza a la Comisión Legal a reunirse con los jefes militares y de inteligencia, a obtener información sobre las prioridades en el ámbito de la inteligencia y a emitir anualmente "estudios de credibilidad y confiabilidad" de carácter reservado[259]. Contrariamente a lo dispuesto en las normas internacionales, la Comisión Legal no está facultada para "investigar y supervisar de forma proactiva las actividades de las entidades que realizan la vigilancia, tener acceso a los resultados

---

[254] Corte IDH, Caso Escher y otros vs. Brasil, serie C, No. 200, *supra,* nota 44, párr. 139 (donde se señala que "las decisiones que adopten los órganos internos que puedan afectar derechos humanos deben estar debidamente motivadas y fundamentadas" y "exponer, a través de una argumentación racional, los motivos en los cuales se fundan, teniendo en cuenta los alegatos y el acervo probatorio aportado a los autos", y se llega a la conclusión de que "el libre convencimiento del juez debe ser ejercido respetándose las garantías adecuadas y efectivas contra posibles ilegalidades y arbitrariedades en el procedimiento en cuestión"). Véase también Informe de 2013 de la Relatora Especial de la CIDH para la Libertad de Expresión*, supra,* nota 78, párr. 165 (donde se indica que la autorización judicial debe "dar cuenta de las razones por las cuales la medida es idónea para alcanzar los fines que persigue en el caso concreto; de si es lo suficientemente restringida para no afectar el derecho involucrado más de lo necesario; y de si resulta proporcional respecto del interés que se quiere promover"); Informe No. 57/19, *supra,* nota 3, párrs. 308 y 312 (donde se refrenda la posición de la Relatora Especial de la CIDH).

[255] Ley de Inteligencia de 2013, *supra,* nota 203, art. 18.

[256] *Id.*

[257] *Id.*, art. 18.4.

[258] *Id.*, art. 21.

[259] *Id.*, arts. 22.1 y 23.

de la vigilancia”[260] o dar a conocer sus conclusiones al público ni está obligada a hacerlo[261]. Por lo tanto, el único órgano externo que ejerce algún tipo de supervisión de las actividades de inteligencia colombianas no es legalmente adecuado.

Por su parte, la Comisión Legal es inoperante. Aunque fue establecida en 2013, varias organizaciones de defensa de los derechos humanos y la prensa han señalado que no funciona en la práctica[262]. En 2017, Dejusticia, la Fundación Karisma y Privacy International informaron que, pese a que se habían reportado casos “sobre la vigilancia ilegal de las comunicaciones de políticos, periodistas y activistas de derechos humanos”, no se había hecho una investigación efectiva de estos incidentes[263]. En mayo de 2020, la prensa colombiana informó que la Comisión Legal no se había reunido formalmente ni había tratado asuntos de inteligencia porque, según el presidente de la Comisión, “[n]o se han podido dar los debates de fondo, justamente porque no hemos podido garantizar la confidencialidad”[264].

Por último, en la Ley de Inteligencia no se requiere que se notifique a las personas sometidas a vigilancia cuando dicha notificación ya no ponga en peligro el propósito de la vigilancia[265]. Una laguna similar llevó al Tribunal Europeo de Derechos Humanos a concluir que la Ley de Inteligencia de Hungría no confería salvaguardias adecuadas[266]. En este caso, el Tribunal rechazó el argumento del Estado de que otras salvaguardias relacionadas con el almacenamiento, el procesamiento y el borrado de datos, así como la posibilidad de que las personas afectadas interpusieran quejas, eran sustitutos suficientes de ese requisito[267]. De manera similar, Colombia tiene una ley de hábeas data que regula el almacenamiento, el procesamiento y el borrado de datos, que se describe con más pormenores en el apartado B.2.b.i. No obstante, en esa ley no se dispone ninguna protección para las personas sometidas a vigilancia con el

---

[260] Informe de 2018 del Alto Comisionado para los Derechos Humanos, *supra,* nota 51, párr. 40; ACNUDH, *Informe anual de la Alta Comisionada de las Naciones Unidas para los Derechos Humanos sobre la situación de los derechos humanos en Colombia*, párr. 25, U.N. Doc. A/HRC/19/21/Add.3 (31 de enero de 2012) [en adelante “Informe de 2012 de la ACNUDH sobre Colombia”] (donde dice que “[l]as débiles facultades de la comisión parlamentaria y la falta de efectividad de los mecanismos existentes de control son dos de los principales retos en la implementación de esta ley”).

[261] Informe de 2018 del Alto Comisionado para los Derechos Humanos, *supra,* nota 51, párr. 40. Véase también TEDH*,* Szabo, App. No. 37138/14, *supra,* nota 128, párr. 82 (donde se dictamina que un informe ministerial sobre el funcionamiento de los servicios de seguridad nacional no constituye una salvaguardia adecuada porque no se da a conocer al público). En cambio, la Oficina del Comisionado con Facultades de Investigar, del Reino Unido, es un órgano independiente encabezado por un Comisionado que tiene la obligación de publicar informes anuales, entre ellos 1) estadísticas relativas al uso de las facultades de investigar; 2) información sobre los resultados de tales usos; 3) información acerca de la aplicación de salvaguardias con respecto a asuntos abarcados por el secreto profesional, material periodístico confidencial y fuentes de información periodística. Investigatory Powers Act 2016, art. 234 (Reino Unido).

[262] Véase KATITZA RODRÍGUEZ PEREDA, ELECTRONIC FRONTIER FOUNDATION, ANÁLISIS COMPARADO DE LAS LEYES Y PRÁCTICAS DE VIGILANCIA EN LATINOAMÉRICA 98 (2016), https://necessaryandproportionate.org/es/comparative-analysis-surveillance-laws-and-practices-latin-america/ (donde dice que la Comisión Legal “actualmente no está operando”); Juan Sebastián Lombo, *El Fantasma de la Comisión de Inteligencia*, EL ESPECTADOR (25 de mayo de 2020), https://www.elespectador.com/noticias/politica/el-fantasma-de-la-comision-de-inteligencia (donde se informa en mayo de 2020 que la Comisión todavía no ha tenido la oportunidad de reunirse formalmente).

[263] DEJUSTICIA, FUNDACIÓN KARISMA AND PRIVACY INTERNATIONAL, EL DERECHO A LA INTIMIDAD EN COLOMBIA. INFORME DE ACTOR INTERESADO. EXAMEN PERIÓDICO UNIVERSAL, 30º PERÍODO DE SESIONES - COLOMBIA, PÁRR. 59 (2017), https://privacyinternational.org/sites/default/files/2018-04/EPU_El%20derecho%20a%20la%20intimidad%20en%20Colombia_2017.pdf [en adelante INFORME DE ACTOR INTERESADO].

[264] *El Fantasma de la Comisión de Inteligencia*, *supra,* nota 262.

[265] TEDH*,* Szabo, App. No. 37138/14, *supra,* nota 128, párr. 86 (donde se requiere la notificación de las personas afectadas en cuanto se pueda efectuar dicha notificación sin poner en peligro el propósito de la vigilancia); TJUE, Asuntos acumulados C-203/15 y C-698/15, Tele2 v. Post-och, *supra,* nota 82, párr. 121.

[266] TEDH*,* Szabo, App. No. 37138/14, *supra,* nota 128, párr. 86.

[267] *Id.*, párr. 87.

propósito de obtener inteligencia, por las razones que se examinan más adelante. En el presente caso, no se notificó oficialmente a los miembros de la CCAJAR que habían sido objeto de vigilancia, quienes se enteraron en cambio por medio de artículos publicados en medios de comunicación, entre ellos uno muy reciente, de 2020[268]. Esto demuestra que, en ausencia de notificación, el Estado ha seguido recopilando y conservando información delicada sobre miembros de la CCAJAR, con lo cual ha puesto en peligro su vida y su trabajo.

b. Las leyes colombianas que regulan el procesamiento, la corrección, el borrado y la transferencia de datos exacerban los riesgos para los miembros de la CCAJAR y sus familiares

El marco jurídico descrito es propenso a los mismos abusos que durante décadas han conducido a la vigilancia de miembros de la CCAJAR y a la retención de datos relacionados con sus comunicaciones y su vida personal durante períodos extraordinariamente prolongados. A pesar de las reiteradas recomendaciones de la Comisión Interamericana y de organismos de las Naciones Unidas, las autoridades de inteligencia han denegado a los miembros de la CCAJAR el acceso a los datos almacenados en los archivos de inteligencia del Estado. Asimismo, el procedimiento establecido en virtud de la Ley de Inteligencia de 2013 para depurar los datos sobre defensores de derechos humanos obtenidos por medio de la vigilancia ilegal resultó ser poco claro e ineficaz. Por último, debido a la falta de protección adecuada contra las transferencias improcedentes al exterior, los datos recopilados por los órganos de inteligencia del Estado son vulnerables a la explotación mundial.

i. Las leyes colombianas no ofrecen ninguna oportunidad a los defensores de derechos humanos para rectificar o borrar los datos recopilados por el Estado acerca de ellos

En la legislación colombiana hay dos mecanismos por medio de los cuales las personas pueden peticionar para que se rectifiquen o se borren los datos de inteligencia acerca de ellos obtenidos de manera indebida por el Estado: la Ley de Hábeas Data de 2012 y el Sistema Nacional de Depuración de Datos y Archivos de Inteligencia y Contrainteligencia. Ninguno de los dos proporciona a los defensores de derechos humanos recursos adecuados, porque el primero excluye toda información recopilada con fines de seguridad nacional, inteligencia o contrainteligencia, y el segundo carece de independencia y transparencia.

La Ley de Hábeas Data regula el derecho de los titulares de los datos a conocer, actualizar y rectificar la información obtenida sobre ellos, pero excluye las bases de datos "que tengan por finalidad la seguridad y defensa nacional" o que "contengan información de inteligencia y contrainteligencia"[269]. Como se señaló en el apartado B.2.a, las autoridades de inteligencia afirman que están facultadas para realizar actividades de vigilancia con fines de "seguridad nacional" y posteriormente asignar a los datos almacenados el carácter de información reservada durante 45 años como máximo[270]. Asimismo, las autoridades de

[268] *Las Carpetas Secretas*, *supra,* nota 31.
[269] Ley 1581 art. 8.a, 18 de octubre de 2012, DIARIO OFICIAL (Colombia) [en adelante "Ley de Hábeas Data de 2012"]; Ley 1712, art. 19.a, 6 de marzo de 2014, DIARIO OFICIAL p. 1 (donde se establece una excepción al derecho de acceso a información relacionada con la "defensa y seguridad nacional").
[270] Ley de Inteligencia de 2013, *supra,* nota 203, art. 33.

inteligencia pueden determinar que la información obtenida por medio de tales actividades de vigilancia es necesaria para la seguridad nacional y, por lo tanto, está exenta de las protecciones conferidas en la Ley de Hábeas Data. Esto infringe la norma internacional ampliamente aceptada de que las personas deben tener la posibilidad de rectificar la información que el Estado ha recopilado sobre ellas[271]. La Comisión Interamericana y los órganos de las Naciones Unidas dedicados a la defensa de los derechos humanos han recordado este requisito a Colombia en reiteradas ocasiones[272]. La Comisión Interamericana ha recomendado a Colombia que "asegure el acceso efectivo del derecho de habeas data para defensoras y defensores con la finalidad de que tengan acceso a sus datos en los archivos de inteligencia y puedan solicitar su corrección, actualización o, en su caso, depuración de los archivos de inteligencia"[273].

En 2010, el Relator Especial de las Naciones Unidas sobre la protección y la promoción de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo recomendó que los Estados estén "legalmente obligados a suprimir o actualizar cualquier información que se haya determinado que no es exacta"[274] y que una institución independiente supervise la depuración de archivos de inteligencia[275]. En 2012, la Alta Comisionada de las Naciones Unidas para los Derechos Humanos observó que "es necesario que se adopten otras medidas para lograr reformar integralmente el sector de inteligencia y transformar la cultura institucional que ha resultado en la comisión de violaciones de derechos humanos"[276] e instó a Colombia a que depurara sus archivos de inteligencia de una manera compatible con las normas de derechos humanos[277].

Colombia no ha cumplido esta obligación. En 2013, por medio de la Ley de Inteligencia se estableció la Comisión Asesora para la depuración de los datos y archivos de inteligencia y contrainteligencia ("la Comisión Asesora"), integrada por autoridades de los sectores público y privado, entre ellas miembros de órganos de inteligencia[278]. La función de la Comisión Asesora era preparar un informe con recomendaciones sobre los criterios de permanencia o retiro de los datos de inteligencia[279]. El Alto Comisionado de las Naciones Unidas para los Derechos Humanos recomendó que estos criterios fueran objeto de un debate público antes de iniciar la depuración[280]. No obstante, cuando concluyó su mandato, la Comisión Asesora no dio a conocer al público esos criterios, con lo cual obstaculizó el escrutinio público del procesamiento y la

---

[271] *Declaración de Principios sobre Libertad de Expresión*, *supra,* nota 192, Principio 3; TJUE, Asunto C-362/14, Schrems v. Data Protection, *supra,* nota 193, párr. 95; Informe de 2010 del Relator Especial sobre la protección y la promoción de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, *supra,* nota 2, párr. 37.

[272] CIDH, *Verdad, justicia y reparación*, *supra,* nota 4, párr. 1188; Informe de 2012 de la ACNUDH sobre Colombia, *supra,* nota 260, párr. 25; ACNUDH, *Informe anual de la Alta Comisionada de las Naciones Unidas para los Derechos Humanos sobre la situación de los derechos humanos en Colombia*, párr. 125, U.N. Doc. A/HRC/4/48 (5 de marzo de 2007).

[273] CIDH, *Capítulo V: Seguimiento de recomendaciones formuladas por la CIDH en sus informes de país o temáticos*, en *Informe Anual 2018*, 579 (2018), https://www.oas.org/es/cidh/docs/anual/2018/docs/IA2018cap.5CO-es.pdf.

[274] Informe de 2010 del Relator Especial sobre la protección y la promoción de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, *supra,* nota 2, Práctica 24.

[275] *Id.*, Práctica 25, párr. 39.

[276] Informe de 2012 de la ACNUDH sobre Colombia, *supra,* nota 260, párr. 26.

[277] *Id.*, párr. 118.e. Véase también Comité de Derechos Humanos, *Examen de los informes presentados por los Estados partes en virtud del artículo 40 del Pacto*, párr. 16, U.N. Doc. CCPR/C/COL/CO/6 (4 de agosto de 2020).

[278] Ley de Inteligencia de 2013, *supra,* nota 203, art. 30.

[279] *Id.*

[280] Informe del ACNUDH de 2017 sobre Colombia, *supra,* nota 217, párr. 83.

rectificación de datos personales por los órganos de inteligencia y las reparaciones de las personas cuyos datos personales se habían obtenido ilegalmente[281].

Después que la Comisión asesora concluyó su mandato, mediante el Decreto 2149 de 2017 se creó el Sistema Nacional de Depuración de Datos y Archivos de Inteligencia y Contrainteligencia ("el Sistema Nacional")[282], "un conjunto de instancias, orientaciones, actividades, recursos, definiciones, programas e instituciones que permiten la aplicación de los principios generales y las disposiciones sobre actualización, corrección y retiro de datos y archivos de inteligencia y contrainteligencia"[283]. Aunque la Comisión Asesora recomendó en su informe al Estado que el órgano de control fuese una "instancia de depuración con carácter civil, autónomo e independiente de los organismos de seguridad y del Gobierno Nacional", la dirección del Sistema Nacional estaba a cargo de funcionarios del Estado, incluso de órganos de inteligencia[284]. Al crear un mecanismo desprovisto de transparencia e independencia, Colombia no cumplió su responsabilidad de asegurar que se borrara la información obtenida por medio de la vigilancia de las comunicaciones de miembros de la CCAJAR.

ii. Las leyes colombianas no proporcionaron suficiente protección contra la transferencia indebida de datos al exterior

La transferencia de información de por sí constituye una injerencia en derechos humanos fundamentales. Por consiguiente, toda norma sobre transferencia de inteligencia, para que sea compatible con las normas internacionales, debe ceñirse a los requisitos de fondo del derecho internacional y a los requisitos procesales a fin de proteger contra el abuso[285]. El Tribunal Europeo de Derechos Humanos, el Comité de Derechos Humanos y los expertos en la materia están de acuerdo en que los mecanismos de transferencia de inteligencia deben estar sometidos a una supervisión eficaz e independiente, además de cumplir los requisitos de legalidad, legitimidad, proporcionalidad y necesidad[286].

---

[281] INFORME DE ACTOR INTERESADO, *supra,* nota 263, párr. 74; PRIVACY INTERNATIONAL, THE STATE OF PRIVACY IN COLOMBIA (26 de enero de 2019), https://privacyinternational.org/state-privacy/58/state-privacy-colombia. Asimismo, antes del establecimiento del Sistema Nacional, las Fuerzas Militares de Colombia informaron al Alto Comisionado de las Naciones Unidas para los Derechos Humanos que habían comenzado a depurar sus archivos de información sobre defensores de derechos humanos y otras personas que habían sido objeto de vigilancia ilegal, lo cual suscitó la preocupación "de que se hayan destruido pruebas de violaciones de los derechos humanos". Informe del ACNUDH de 2017 sobre Colombia, *supra,* nota 217, párr. 83.

[282] Decreto 2149, 20 de diciembre de 2017, DIARIO OFICIAL (Colombia).

[283] *Id*., art. 2.2.3.12.1.1.

[284] Gustavo Gallon, *Inteligencia en Beneficio del Gobierno y de Toda la Sociedad*, EL ESPECTADOR (6 de mayo de 2020), https://www.elespectador.com/opinion/columnistas/gustavo-gallon/inteligencia-en-beneficio-del-gobierno-y-de-toda-la-sociedad-column-918263/.

[285] Dictamen 1/15, Proyecto de Acuerdo entre Canadá y la Unión Europea, ECLI:EU:C:2017:592, párr. 125 (26 de julio de 2017); TEDH, Big Brother Watch, App. No. 58170/13, *supra,* nota 123, párr. 362; Informe de 2018 del Alto Comisionado para los Derechos Humanos, *supra,* nota 51, párr. 21; Comité de Derechos Humanos, *Concluding observations on the Seventh Periodic Report of Sweden*, párr. 37, U.N. Doc. CCPR/C/SWE/CO/7 (28 de abril de 2016).

[286] TEDH, Big Brother Watch, App. No. 58170/13, *supra,* nota 123, párr. 362 (donde se señala que la transmisión de datos recopilados por medio de interceptación a gran escala también debería ser objeto de un control independiente); TEDH, Szabo, App. No. 37138/14, *supra,* nota 128, párrs. 78 y 79 (donde se afirma que la transferencia y el intercambio entre gobiernos de inteligencia obtenida por medio de vigilancia secreta requería la atención particular de medidas correctivas y de supervisión externas); Comité de Derechos Humanos, *Concluding observations on the Initial Report of Pakistan*, párr. 35, U.N. Doc. CCPR/C/PAK/CO/1 (23 de agosto de 2017) [en adelante *HRC Concluding Observations on Pakistan*] (donde se expresa preocupación por la ley pakistaní que dispone el intercambio de información y la cooperación con gobiernos de otros países sin

El Comité de Derechos Humanos ha reconocido que las medidas relativas al intercambio de inteligencia deben estar supeditadas a autorización judicial previa y a supervisión independiente[287]. El Tribunal Europeo de Derechos Humanos ha dispuesto también 1) que en las leyes internas se indiquen claramente las circunstancias en las cuales puedan transferirse datos a otros países; 2) que el Estado que efectúe la transferencia se cerciores de que el Estado receptor cuente con salvaguardias adecuadas contra los abusos, y 3) que haya salvaguardias más estrictas para la transferencia de material sometido a reserva especial; por ejemplo, con contenido periodístico[288]. Por último, el Tribunal de Justicia de la Unión Europea ha reconocido la importancia de notificar a las personas cuyos datos se proporcionen a gobiernos de otros países, a fin de asegurar el respeto de la vida privada[289].

Hay indicios que Colombia ha proporcionado información personal obtenida de manera ilegal, incluso información relacionada con la CCAJAR, a gobiernos de otros países, lo cual no es permisible. Las leyes colombianas confieren a las autoridades del país facultades discrecionales excesivas para proveer información obtenida por medio de prácticas abusivas de vigilancia de las comunicaciones.

De hecho, las leyes y las normas colombianas contienen muy poca información sobre la forma en que Colombia monitorea y examina la idoneidad de las leyes en materia de protección de datos de otros países con los cuales intercambia datos, lo cual es preocupante. El título VIII de la Ley de Hábeas Data rige la transferencia de datos a terceros países. De acuerdo con la ley, "[s]e prohíbe la transferencia de datos personales de cualquier tipo a países que no proporcionen niveles adecuados de protección de datos" y se faculta a la Superintendencia de Industria y Comercio para declarar la conformidad[290]. No obstante, como se señala en la Circular Externa No. 005 de 2017 de la Superintendencia, Colombia considera que Estados Unidos, país ampliamente criticado porque no protege los datos personales de extranjeros, cuenta con un nivel adecuado de protección de los datos[291]. Ni en la Ley de Hábeas Data ni en la Circular se describen las circunstancias en que pueden efectuarse las transferencias. No se requiere que las autoridades demuestren, antes de transferir los datos, que este intercambio es compatible con los principios de legalidad, legitimidad, necesidad y proporcionalidad. Tampoco se requiere autorización o supervisión alguna de los datos que se transfieran ni la notificación de las

autorización o supervisión judicial); *Observaciones finales del Comité de Derechos Humanos sobre el Reino Unido*, *supra,* nota 155, párr. 24.c (donde se afirma que el Reino Unido debe "[v]elar por que existan sistemas de supervisión estricta de la vigilancia, interceptación e intercambio con organismos de inteligencia de las actividades de comunicación personal, entre otras cosas previendo la intervención judicial en la autorización de tales medidas en todos los casos"); Informe de 2019 del Relator Especial sobre el derecho a la privacidad, *supra,* nota 36, párrs. 9 y 10, n. 17 (donde se alienta a los Estados a que "modifiquen sus leyes para que los organismos independientes de supervisión de su territorio estén facultados para consultar con sus homólogos en otros Estados y a que hagan un seguimiento de todos los casos en los que se hayan intercambiado datos con otro Estado, [...] independientemente de si esos datos se encuentran en el Estado de origen o en el de destino").

[287] *HRC Concluding Observations on Pakistan*, *supra,* nota 286, párr. 35; *Observaciones finales del Comité de Derechos Humanos sobre el Reino Unido*, *supra,* nota 155, párr. 24.

[288] TEDH, Big Brother Watch, App. No. 58170/13, *supra,* nota 123, párr. 362.

[289] TJUE, Dictamen 1/15, *supra*, nota 285, párr. 220 (donde se requiere la notificación de las personas cuyos datos se intercambien entre gobiernos).

[290] Ley de Hábeas Data de 2012, *supra,* nota 269, párr. 26.

[291] Superintendencia de Industria y Comercio, *Circular Externa No. 005*, párr. 3.2, 10 de agosto de 2017, https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/Circular_Externa_5_Ago_10_2017.pdf. Véase DEJUSTICIA, RESPONSE TO CALL FOR INPUTS ON HUMAN RIGHTS CHALLENGES RELATING TO THE RIGHT TO PRIVACY IN THE DIGITAL AGE IN COLOMBIA 10, n. 6 (2018), https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/Dejusticia.pdf (donde se describe la insuficiencia de las normas de Colombia en materia de transferencia de datos).

personas cuyos datos se intercambien, y no se disponen recursos para las personas cuyos datos han sido transferidos. Por todas estas razones, las leyes de Colombia sobre intercambio de datos no son compatibles con las normas internacionales fundamentales.

V. CONCLUSIÓN

Por las razones expuestas anteriormente, y por medio de este *amici curiae*, ARTICLE 19, Electronic Frontier Foundation, la Fundación Karisma y Privacy International instan a la Corte Interamericana de Derechos Humanos a que determine que el marco jurídico actual de Colombia que regula las actividades de inteligencia, así como la vigilancia ilegal y arbitraria de miembros de la CCAJAR y sus familiares realizada por las autoridades colombianas, violan los artículos 4 (derecho a la vida), 5 (derecho a la integridad personal), 8 (garantías judiciales), 11 (protección de la honra y de la dignidad), 13 (libertad de pensamiento y de expresión), 16 (libertad de asociación), 19 (derechos del niño), 22 (derecho de circulación y de residencia) y 25 (protección judicial) de la Convención Americana sobre Derechos Humanos.

Fecha: 24 de mayo de 2022

Atentamente,

Roxanna Altholz
Codirectora
International Human Rights Law Clinic
Berkeley Law
Asesor Jurídico de Amici Curiae

Astha Sharma Pokharel
Docente
International Human Rights Law Clinic
Berkeley Law
Asesor Jurídico de Amici Curiae